

# HP StorageWorks

## Enterprise File Services WAN Accelerator 2.1.5

### deployment guide



\*407118-002\*

Part number: 407118-002  
Second edition: June 2006



## **Legal and notice information**

© Copyright 2006 Hewlett-Packard Development Company, L.P.

© Copyright 2003–2006 Riverbed Technology, Inc.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Linux is a trademark of Linus Torvalds in the United States and in other countries.

Microsoft, Windows, Windows NT, Windows 2000, Outlook, and Windows Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and in other countries.

UNIX is a registered trademark in the United States and in other countries, exclusively licensed through X/Open Company, Ltd.

Parts of this product are derived from the following software:

Apache © 2000-2003 The Apache Software Foundation. All rights reserved.

bsdstr.c, © 1998 Todd C. Miller (Todd.Miller@courtesan.com). All rights reserved.

Busybox, © Eric Andersen

Less © 1984-2002 Mark Nudelman

Libevent, © 2000-2002 Niels Provos. All rights reserved.

LibGD, Version 2.0 licensed by Boutell.Com, Inc.

Libtecla, © 2000, 2001 by Martin C. Shepherd. All rights reserved.

Linux Kernel, © Linus Torvalds

md5, md5.cc, © 1995 University of Southern California. All rights reserved. © 1991-2, RSA Data Security, Inc. All rights reserved.

my\_getopt.{c,h}, © 1997, 2000, 2001, 2002, Benjamin Sittler. All rights reserved.

NET-SNMP: © 1989, 1991, 1992 by Carnegie Mellon University. All rights reserved.

OpenSSH, © 2002 Nils Nordman. All rights reserved.

ptmalloc © 2001 Wolfram Gloger

SMTP, © Mark Ryan, Hugo Haas, Christoph Lameter, and Dave Collier-Brown

Vixie-Cron, © 1988, 1990, 1993, 1994 by Paul Vixie. All rights reserved.

Zile, © 1997-2001 Sandro Sigalam © 2003 Reuben Thomas. All rights reserved.

For detailed copyright and license agreements, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*. For modified source code (where required), see the HP technical support site at .

Certain libraries were used in the development of this software, licensed under GNU Lesser General Public License, Version 2.1, February 1999. For the copyright and license agreement, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*. For a list of libraries and source material (where required), see the HP technical support site at <http://www.hp.com>.

# Contents

<b>Introduction</b>	.....	<b>1</b>
About This Guide.....		1
Types of Users .....		1
Organization of This Guide .....		2
Document Conventions .....		3
Hardware and Software Dependencies .....		4
Ethernet Network Compatibility.....		4
Antivirus Compatibility .....		4
Additional Resources .....		5
Related HP Documentation .....		6
Online Documentation.....		6
Related Reading.....		6
Contacting HP .....		7
Technical Support.....		7
HP Storage Web Site.....		7
<b>Chapter 1    Designing an HP EFS WAN Accelerator Deployment</b>	.....	<b>9</b>
Introduction to the HP EFS WAN Accelerator .....		9
Transaction Acceleration.....		10
Scalable Data Referencing .....		10
Virtual Window Expansion .....		10
Transaction Prediction.....		11
Design and Deployment Overview.....		11
Definition of Terms.....		13
Bypass Mode.....		13
Failover Mode.....		14
<b>Chapter 2    In-Path Deployments</b>	.....	<b>17</b>
Introduction to Physical In-Path Deployments .....		18

In-Path, Failover Support Deployment .....	18
Basic Steps (Client-Side).....	18
Basic Steps (Server-Side) .....	20
In-Path, Two Routing Points Deployment .....	20
Basic Steps (Client-Side).....	21
Basic Steps (Server-Side) .....	21
In-Path, Server-Side Deployment.....	21
Basic Steps (Client-Side).....	22
Basic Steps (Server-Side) .....	22
In-Path, Server-Side, One to One Deployment.....	22
Basic Steps (Client-Side).....	23
Basic Steps (Server-Side) .....	23
<b>Chapter 3 Virtual In-Path Network Deployments ..... 25</b>	
Introduction to Virtual In-Path Deployments .....	25
In-Path, Load Balanced, Layer-4 Switch.....	26
Basic Steps (Client-Side).....	27
Basic Steps (Server-Side) .....	27
<b>Chapter 4 Out-of-Path Network Deployments ..... 29</b>	
Introduction to Out-of-Path Deployments .....	29
Out-of-Path, Failover Deployment .....	30
Basic Steps (Client-Side).....	31
Basic Steps (Server-Side) .....	33
Out-of-Path, Static Cluster Deployment .....	33
Basic Steps (Client-Side).....	33
Basic Steps (Server-Side) .....	35
Hybrid: In-Path and Out-of-Path Deployment.....	35
Basic Steps (Client-Side).....	35
Basic Steps (Server-Side) .....	37
<b>Chapter 5 Configuring Connection Forwarding ..... 39</b>	
Introduction to Connection Forwarding.....	39
Neighbors in Connection Forwarding .....	40
Load-Balancing .....	40
One-to-One Failover Deployment .....	41
Configuring Connection Forwarding .....	41
Configuring Connection Forwarding Using the Management Console .....	42
Basic Steps (Client-Side) .....	42
Basic Steps (Server-Side).....	42
Configuring Connection Forwarding Using the CLI.....	44

<b>Chapter 6 Policy-Based Routing Deployments .....</b>	<b>45</b>
Introduction to PBR .....	46
Overview of CDP.....	46
How PBR works on a Cisco 6500 Platform, Version 12.2(17d) SXB1 .....	47
Connecting the HP EFS WAN Accelerator to Your Network in PBR Deployments.....	48
Asymmetric HP EFS WAN Accelerator Deployments With PBR.....	49
Configuring PBR Using the CLI .....	49
Configuring PBR Using the Management Console .....	51
Client-Side HP EFS WAN Accelerator Attached to a Router through a Switch .....	54
Basic Steps (Client-Side).....	54
Basic Steps (Server-Side) .....	54
Client-Side HP EFS WAN Accelerator Attached to an Inside Router.....	55
Basic Steps (Client-Side).....	55
Basic Steps (Server-Side) .....	55
PBR Between VLANs .....	55
Symmetric HP EFS WAN Accelerator Deployments With PBR and Autodiscovery .....	57
Symmetric Deployments with PBR, Autodiscovery, and CDP .....	60
Troubleshooting .....	62
<b>Chapter 7 WCCP Deployments .....</b>	<b>63</b>
Introduction to WCCP .....	64
Basic Steps.....	65
WCCP CLI Commands .....	66
Connecting the HP EFS WAN Accelerator to Your Network in WCCP Deployments.....	67
A Basic WCCP Configuration .....	68
Connecting the HP EFS WAN Accelerator .....	68
Configuring the WCCP Router or Multi-Layer Switch .....	68
Configuring the Client-Side HP EFS WAN Accelerator.....	69
Configuring WCCP Using the Management Console .....	70
Basic Steps (Client-Side).....	70
Basic Steps (Server-Side) .....	75
Dual WCCP Deployment.....	76
Additional WCCP Features.....	79
Security.....	79
Multicast .....	80
TCP Port Redirection .....	80

Specific Traffic Redirection .....	81
Load Balancing.....	81
Failover Support .....	81
Troubleshooting .....	82
<b>Chapter 8 Proxy File Service Deployments .....</b>	<b>83</b>
Introduction to PFS .....	83
PFS Terms.....	84
PFS Operating Modes .....	85
How Does PFS Work? .....	86
When to Use PFS .....	87
When to use Global Mode.....	88
Configuration Checklist for PFS .....	88
Configuring PFS Using the Management Console.....	89
<b>Chapter 9 RADIUS and TACACS+ Authentication .....</b>	<b>97</b>
Introduction to Authentication.....	97
Configuring a RADIUS Server with FreeRADIUS .....	98
Configuring a TACACS+ Server with Free TACACS+.....	100
Configuring RADIUS Authentication in the HP EFS WAN Accelerator.....	101
Configuring RADIUS Authentication.....	101
Basic Steps.....	102
Configuring TACACS+ Authentication in the HP EFS WAN Accelerator.....	103
Configuring TACACS+ Authentication.....	103
Basic Steps.....	104
<b>Chapter 10 Serial Cluster and Cascade Deployments .....</b>	<b>107</b>
Serial Cluster Deployment.....	107
A Basic Serial Cluster Deployment.....	109
Cascade Deployment .....	111
Peering Rules.....	111
Fixed-Target Rules .....	112
<b>Glossary .....</b>	<b>113</b>
<b>Index .....</b>	<b>117</b>

# Introduction

## In This Introduction

Welcome to the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*. Read this introduction for an overview of the information provided in this guide and for an understanding of the documentation conventions used throughout. This introduction contains the following sections:

- ◆ “About This Guide,” next
- ◆ “Hardware and Software Dependencies” on page 4
- ◆ “Ethernet Network Compatibility” on page 4
- ◆ “Antivirus Compatibility” on page 4
- ◆ “Additional Resources” on page 5
- ◆ “Contacting HP” on page 7

---

## About This Guide

The *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide* describes how to configure the HP StorageWorks Enterprise File Services WAN Accelerator (HP EFS WAN Accelerator) in complex in-path and out-of-path deployments such as failover, multiple routing points, static clusters, connection forwarding, Web Cache Communication Protocol (WCCP), Layer -4 and Policy-Based Routing (PBR), and Proxy File Service (PFS).

## Types of Users

This guide is written for storage and network administrators with familiarity administering and managing networks using Common Internet File System (CIFS), Hypertext Transport Protocol (HTTP), File Transfer Protocol (FTP), and Microsoft Exchange.

## **Organization of This Guide**

The *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide* includes the following chapters:

- ◆ [Chapter 1, “Designing an HP EFS WAN Accelerator Deployment,”](#) describes the HP EFS WAN Accelerator and provides an overview of how it works. It also describes how to design and deploy the HP EFS WAN Accelerator in your network.
- ◆ [Chapter 2, “In-Path Deployments,”](#) describes physical in-path deployments.
- ◆ [Chapter 3, “Virtual In-Path Network Deployments,”](#) describes virtual in-path deployments.
- ◆ [Chapter 4, “Out-of-Path Network Deployments,”](#) describes out-of-path deployments.
- ◆ [Chapter 5, “Configuring Connection Forwarding,”](#) describes how to configure the HP EFS WAN Accelerator to forward connections in asymmetric networks.
- ◆ [Chapter 6, “Policy-Based Routing Deployments,”](#) describes how to configure the HP EFS WAN Accelerator for deployments using PBR, Cisco Discovery Protocol (CDP), and autodiscovery.
- ◆ [Chapter 7, “WCCP Deployments,”](#) describes how to configure the HP EFS WAN Accelerator and routers for WCCP.
- ◆ [Chapter 8, “Proxy File Service Deployments,”](#) describes how to configure the HP EFS WAN Accelerator to perform PFS.
- ◆ [Chapter 9, “RADIUS and TACACS+ Authentication,”](#) how to configure Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) authentication for the HP EFS WAN Accelerator.
- ◆ [Chapter 10, “Serial Cluster and Cascade Deployments,”](#) describes how to configure the HP EFS WAN Accelerator in serial and cascade clusters to increase optimization.

A glossary of terms follows the chapters, and a comprehensive index directs you to areas of particular interest.

## Document Conventions

This manual uses the following standard set of typographical conventions to introduce new terms, illustrate screen displays, describe command syntax, and so forth.

Convention	Meaning
<i>italics</i>	Within text, new terms and emphasized words appear in italic typeface.
<b>boldface</b>	Within text, commands, keywords, identifiers (names of classes, objects, constants, events, functions, program variables), environment variables, filenames, Graphical User Interface (GUI) controls, and other similar terms appear in bold typeface.
<b>Courier</b>	Information displayed on your terminal screen and information that you are instructed to enter appear in Courier font.
<b>KEYSTROKE</b>	Keys that you are to press appear in uppercase letters in Helvetica font.
<b>&lt;&gt;</b>	Within syntax descriptions, values that you specify appear in angle brackets. For example: <b>interface &lt;ipaddress&gt;</b>
<b>[ ]</b>	Within syntax descriptions, optional keywords or variables appear in brackets. For example: <b>ntp peer &lt;addr&gt; [version &lt;number&gt;]</b>
<b>{ }</b>	Within syntax descriptions, required keywords or variables appear in braces. For example: <b>{delete &lt;filename&gt;   upload &lt;filename&gt;}</b>
<b> </b>	Within syntax descriptions, the pipe symbol represents a choice to select one keyword or variable to the left or right of the symbol. (The keyword or variable can be either optional or required.) For example: <b>{delete &lt;filename&gt;   upload &lt;filename&gt;}</b>

---

## Hardware and Software Dependencies

The following table summarizes the hardware and software requirements for the HP EFS WAN Accelerator.

HP Component	Hardware and Software Requirements
<b>HP EFS WAN Accelerator</b>	<ul style="list-style-type: none"><li>• 19 inch (483 mm) two or four-post rack.</li></ul>
<b>HP EFS WAN Accelerator Management Console, EFS WAN Accelerator Manager</b>	<ul style="list-style-type: none"><li>• Any computer that supports a Web browser with a color image display.</li><li>• The Management Console has been tested with Firefox, version 1.0.x and 1.5.x and Microsoft Internet Explorer, version 6.0x.</li></ul> <p>NOTE: Javascript and cookies must be enabled in your Web browser.</p>

---

## Ethernet Network Compatibility

The HP EFS WAN Accelerator supports the following types of Ethernet networks:

- ◆ Ethernet Logical Link Control (LLC) (IEEE 802.2 - 2002)
- ◆ Fast Ethernet 100 Base-TX (IEEE 802.3 - 2002)
- ◆ Gigabit Ethernet over Copper 1000 Base-T and Fiber 1000 Base-SX (LC connector) (IEEE 802.3 - 2002)

The Primary port in the HP EFS WAN Accelerator is 10 Base-T/100, Base-TX/1000, and Base-T/SX Mbps (IEEE 802.3 -2002).

In-path HP EFS WAN Accelerator ports are 10/100/1000 Base-TX or Gigabit Ethernet 1000Base-T/SX (IEEE 802.3 – 2002) (depending on your order).

The HP EFS WAN Accelerator supports Virtual Local Area Network (VLAN) Tagging (IEEE 802.1Q - 2003). It does not support the Cisco InterSwitch Link (ISL) protocol.

All copper interfaces are auto-sensing for speed and duplex (IEEE 802.3 - 2002).

The HP EFS WAN Accelerator auto-negotiates speed and duplex mode for all data rates and supports full duplex mode and flow control (IEEE 802.3 – 2002).

The HP EFS WAN Accelerator with a Gigabit Ethernet card supports Jumbo Frames on in-path and primary ports.

---

## Antivirus Compatibility

The HP EFS WAN Accelerator has been tested with the following antivirus software with no impact on performance:

- ◆ Network Associates (McAfee) VirusScan 7.0.0 Enterprise on the server
- ◆ Network Associates (McAfee) VirusScan 7.1.0 Enterprise on the server
- ◆ Network Associates (McAfee) VirusScan 7.1.0 Enterprise on the client
- ◆ Symantec (Norton) AntiVirus Corporate Edition 8.1 on the server

The HP EFS WAN Accelerator has been tested with the following antivirus software with a noticeable to moderate impact on performance:

- ◆ F-Secure Anti-Virus 5.43 on the client
- ◆ F-Secure Anti-Virus 5.5 on the server
- ◆ Network Associates (McAfee) NetShield 4.5 on the server
- ◆ Network Associates VirusScan 4.5 for multi-platforms on the client
- ◆ Symantec (Norton) AntiVirus Corporate Edition 8.1 on the client

---

## Additional Resources

- ◆ This section describes resources that supplement the information in this guide. It contains the following sections:
  - ◆ “[Related HP Documentation](#)” on page 6
  - ◆ “[Online Documentation](#)” on page 6
  - ◆ “[Related Reading](#)” on page 6

## **Related HP Documentation**

You can access the complete document set for the HP EFS WAN Accelerator from the *HP StorageWorks EFS WAN Accelerator Documentation Set CD-ROM*:

- ◆ *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide* describes how to install and configure the HP EFS WAN Accelerator.
- ◆ *HP Enterprise File Services WAN Accelerator Management Console User Guide* describes how to manage and administer an HP EFS WAN Accelerator using the Management Console.
- ◆ *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual* is a reference manual for the HP EFS WAN Accelerator command-line interface. It lists commands, syntax, parameters, and example usage.
- ◆ *HP StorageWorks Enterprise File Services WAN Accelerator Manager User's Guide* describes how to install, configure, and administer a network made up of multiple HP EFS WAN Accelerators using the EFS WAN Accelerator Manager.
- ◆ *HP Enterprise File Services Remote Copy Utility Reference Manual* describes how to install and deploy the HP EFS Remote Copy Utility (HP EFS RCU). The HP EFS RCU is an optional utility of the HP EFS WAN Accelerator that copies, mirrors, and transparently prepopulates data. You can download the HP EFS RCU from the HP support site located at <http://www.hp.com>.
- ◆ *HP StorageWorks Enterprise File Services WAN Accelerator Bypass NIC Installation Guide* describes how to install bypass cards in the HP EFS WAN Accelerator.

## **Online Documentation**

The HP EFS WAN Accelerator documentation set is periodically updated with new information. To access the most current version of the HP EFS WAN Accelerator documentation and other technical information, go to <http://www.hp.com/support/manuals>.

## **Related Reading**

To learn more about network administration, consult the following books:

- ◆ *Microsoft Windows 2000 Server Administrator's Companion* by Charlie Russell and Sharon Crawford (Microsoft Press, 2000)
- ◆ *Common Internet File System (CIFS) Technical Reference* by the Storage Networking Industry Association (Storage Networking Industry Association, 2002)
- ◆ *TCP/IP Illustrated, Volume I, The Protocols* by W. R. Stevens (Addison-Wesley, 1994)
- ◆ *Internet Routing Architectures (2nd Edition)* by Bassam Halabi (Cisco Press, 2000)

## Technical Support

### Contacting HP

This section describes how to contact HP.

Telephone numbers for worldwide technical support are listed on the following HP web site: <http://www.hp.com/support>. From this web site, select the country of origin. For example, the North American technical support number is 800-633-3600.

---

**NOTE:** For continuous quality improvement, calls may be recorded or monitored.

---

Be sure to have the following information available before calling:

- ◆ Technical support registration number (if applicable)
- ◆ Product serial numbers
- ◆ Product model names and numbers
- ◆ Applicable error messages
- ◆ Operating system type and revision level
- ◆ Detailed, specific questions

---

### HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access the storage site at: <http://www.hp.com/country/us/eng/prodserv/storage.html>. From this web site, select the appropriate product or solution.



## CHAPTER 1

# Designing an HP EFS WAN Accelerator Deployment

## In This Chapter

This chapter describes how the HP EFS WAN Accelerator works and how to design an HP EFS WAN Accelerator deployment. This chapter includes the following sections:

- ◆ “[Introduction to the HP EFS WAN Accelerator](#)” next
- ◆ “[Design and Deployment Overview](#)” on page 11
- ◆ “[Definition of Terms](#)” on page 13
- ◆ “[Bypass Mode](#)” on page 13
- ◆ “[Failover Mode](#)” on page 14

---

## Introduction to the HP EFS WAN Accelerator

The causes for slow throughput in Wide Area Networks (WANs) are well known: high delay (round-trip time or latency), limited bandwidth, and chatty application protocols. Virtually all large enterprises spend a significant portion of their information technology budgets on storage and networks, much of it spent to compensate for slow throughput by deploying redundant servers and storage, and the required backup equipment. HP EFS WAN Accelerators enable you to consolidate and centralize key IT resources to save money, reduce capital expenditures, simplify key business processes, and improve productivity.

The HP EFS WAN Accelerator not only addresses the bandwidth problem and application protocol chattiness but the latency problem as well. The HP EFS WAN Accelerator uses Transaction Acceleration (TA) to optimize throughput and save bandwidth on WANs.

HP EFS WAN Accelerators intercept client-server connections without interfering with normal client-server interactions, file semantics, or protocols. All client requests are passed through to the server normally, while relevant traffic is optimized to improve performance. HP EFS WAN Accelerators can be easily introduced into an enterprise environment without requiring any significant changes to the network or architecture.

## **Transaction Acceleration**

Transaction Acceleration (TA) is composed of the following optimization mechanisms:

- ◆ A connection bandwidth-reducing mechanism called Scalable Data Referencing (SDR).
- ◆ A Virtual TCP Window Expansion (VWE) mechanism that repacks TCP payloads with references that represent arbitrary amounts of data.
- ◆ A latency reduction and avoidance mechanism called Transaction Prediction (TP).

SDR and TP can work independently or in conjunction with one another depending on the characteristics and workload of the data sent across the network. The results of the optimization vary, but typically result in throughput improvements in the range of 10 to 100 times over unaccelerated links.

## **Scalable Data Referencing**

Bandwidth optimization is delivered through Scalable Data Referencing (SDR). SDR uses a proprietary algorithm to break up Transmission Control Protocol (TCP) data streams into *data chunks* that are stored in the hard disk (*data store*) of the HP EFS WAN Accelerator. Each data chunk is assigned a unique integer label (*reference*) before it is sent to the peer HP EFS WAN Accelerator across the WAN. If the same byte sequence is seen again in the TCP data stream, then the reference is sent across the WAN instead of the raw data chunk. The peer HP EFS WAN Accelerator uses this reference to reconstruct the original data chunk and the TCP data stream. Data and references are maintained in persistent storage in the *data store* within each HP EFS WAN Accelerator. There are no consistency issues even in the presence of replicated data.

### **How Does SDR Work?**

When data is sent for the first time across a network (no commonality with any file ever sent before), all data and references are *new* and are sent to the HP EFS WAN Accelerator on the far side of the network. This new data and the accompanying references are compressed using conventional algorithms, when and if, it improves performance.

When data is changed, new data and references are created. Thereafter, whenever new requests are sent across the network, the references created are compared with those that already exist in the local data store. Any data that already exists on the far side of the network are not sent—only the references are sent across the network.

As files are copied, edited, renamed, and otherwise changed or moved, the HP EFS WAN Accelerator continually builds out the data store to include more and more data and references. References can be shared by different files and by files in different applications if the underlying bits are common to both.

## **Virtual Window Expansion**

Virtual TCP Window Expansion (VWE) allows HP EFS WAN Accelerators to repack TCP payloads with references that represent arbitrary amounts of data. This is possible because unlike other compression products, HP EFS WAN Accelerators operate at the application layer and terminate TCP, which gives them more flexibility in the way they optimize WAN traffic.

Essentially, the TCP payload is increased from its normal 64 kilobytes to an arbitrarily large amount. Because of this increased payload, a given application that relies on TCP performance (for example, Hypertext Transfer Protocol or File Transfer Protocol) takes fewer trips across the WAN to accomplish the same task. When HP EFS WAN Accelerators are deployed in a network, many applications run 10 to 100 times faster.

## Transaction Prediction

Latency optimization is delivered through Transaction Prediction (TP). TP involves an intimate understanding of protocol semantics to reduce the chattiness that would normally occur over the WAN. By acting on foreknowledge of specific protocol request-response mechanisms, HP EFS WAN Accelerators streamline the delivery of data that would normally be delivered in small increments through large numbers of handshakes and interactions between the client and server over the WAN. As transactions are executed between the client and server, the HP EFS WAN Accelerators intercept each transaction, compare it to the database of past transactions, and make decisions about the probability of future events.

Based on this model, if an HP EFS WAN Accelerator determines there is a high likelihood of a future transaction occurring, it performs that transaction rather than waiting for the response from the server to propagate back to the client and then back to the server. Dramatic performance improvements result from the time saved by not waiting for each serial transaction to arrive prior to making the next request. Instead, the transactions are pipe-lined one right after the other.

Of course, transactions are only executed by HP EFS WAN Accelerators ahead of the client when it is safe to do so. To ensure data integrity, HP EFS WAN Accelerators are designed with knowledge of the underlying protocols (for example, Common Internet File System (CIFS) oplocks) to know precisely when, and if, it is safe to do so. Fortunately, a wide range of common applications have very predictable behaviors and, consequently, TP can enhance WAN performance significantly. When combined with SDR, TP improves overall WAN performance up to 100 times.

---

## Design and Deployment Overview

The following section summarizes the factors you need to consider before deploying the HP EFS WAN Accelerator in your network.

When you deploy the HP EFS WAN Accelerator, you must consider the following elements for both the client and server-side of your network.

**1. Determine what kind of site you have:**

- ◆ **User Locations.** A branch office that has users but no servers accessed by the other sites. Typically, a user location is a branch office at a remote site that accesses data from a headquarters or data center.
- ◆ **Server Locations.** A central server location that remote offices access data from. Typically, a server location is a data center serving branch offices or regional offices that access data that is centrally located.

- ◆ **Users and Servers.** A site that has users and servers that are accessed remotely. Typically, users and servers are in a regional office with branch offices at remote sites that access data from remote sites and a data center.

2. Determine what kind of WAN routing infrastructure you have. For example, do you have one or two WAN routers?
3. How much bandwidth do you use? If you use large amounts of bandwidth, you need to consider deploying multiple HP EFS WAN Accelerators using a Layer-4 switch, Web Cache Communication Protocol (WCCP), or deploying HP EFS WAN Accelerators in a static cluster.
4. Choose a network template:
  - ◆ **Physical In-Path.** In a physical in-path deployment the HP EFS WAN Accelerator is physically in the direct path between clients and servers. The clients and servers continue to see client and server Internet Protocol (IP) addresses. Physical in-path configurations are suitable for any location where the total bandwidth is within the limits of the installed HP EFS WAN Accelerator. For detailed information, see [Chapter 2, “In-Path Deployments.”](#)
  - ◆ **Virtual In-Path.** In a virtual in-path deployment the HP EFS WAN Accelerator is virtually in the path between clients and servers. In a virtual in-path deployment, clients and servers continue to see client and server IP addresses. This deployment differs from a physical in-path deployment in that a packet redirection mechanism is used to direct packets to HP EFS WAN Accelerators that are not in the physical path of the client or server. Redirection mechanisms include Layer-4 switches, Web Cache Communication Protocol (WCCP), and Policy-Based Routing (PBR). For detailed information, see [Chapter 3, “Virtual In-Path Network Deployments.”](#)
  - ◆ **Out-of-Path.** In an out-of-path deployment the HP EFS WAN Accelerator is not in the direct path between the client and the server. In an out-of-path deployment, the HP EFS WAN Accelerator acts as a proxy. An out-of-path configuration is suitable for data center locations where physical in-path or virtual in-path configurations are not possible. For detailed information, see [Chapter 4, “Out-of-Path Network Deployments.”](#)
5. Determine how many HP EFS WAN Accelerators you need for your site:
  - ◆ One HP EFS WAN Accelerator is typically deployed in network environments with small to moderate bandwidth requirements.
  - ◆ Two HP EFS WAN Accelerators are deployed for redundancy in network environments where network outages cannot be tolerated.
  - ◆ Two HP EFS WAN Accelerators are deployed in network environments with multiple WAN links.
  - ◆ Multiple HP EFS WAN Accelerators are deployed in cluster configurations.
6. Do you have a firewall?

---

## Definition of Terms

The following terms are used to describe features, attributes, and processes in the HP EFS WAN Accelerator:

- ◆ **Optimization.** The process of increasing data throughput and network performance over the WAN using the HP EFS WAN Accelerator. An optimized connection exhibits bandwidth reduction as it traverses the WAN.
- ◆ **Scalable Data Referencing (SDR).** The proprietary algorithms that allow an arbitrarily large amount of data to be represented by a small number of references to the HP EFS WAN Accelerator data store. As data flows through the HP EFS WAN Accelerator, all TCP traffic is mapped onto references to data that is stored on either side of the link. This technology increases WAN network performance and decreases consumed bandwidth.
- ◆ **Auto-discovery.** Auto-discovery is the process by which the HP EFS WAN Accelerator automatically intercepts and optimizes traffic on all Internet Protocol (IP) addresses and ports. By default, auto-discovery is applied to all IP addresses and the ports which are not secure or interactive.
- ◆ **Fixed-Target.** Fixed target rules directly specify out-of-path HP EFS WAN Accelerators near the target server that you want to optimize. You determine which servers you would like the HP EFS WAN Accelerator to optimize (and, optionally, which ports), and add fixed-target rules to specify the network of servers, ports, and out-of-path HP EFS WAN Accelerators to use.
- ◆ **Pass-Through.** Pass-through describes WAN traffic that traverses the network unoptimized. You define pass-through rules to exclude subnets from optimization. Traffic is also passed through when the HP EFS WAN Accelerator is in bypass mode. Pass-through might be due to in-path rules or because the connection was established before the HP EFS WAN Accelerator was put in place or before the HP EFS WAN Accelerator service was enabled.
- ◆ **Bypass.** The HP EFS WAN Accelerator is equipped with a bypass interface to prevent a single point of failure. If there is a serious problem with the HP EFS WAN Accelerator or it is not powered on, it goes into bypass mode and the traffic is passed-through unoptimized.
- ◆ **Failover.** You can deploy redundant HP EFS WAN Accelerators in your network to ensure optimization continues if there is a failure in one of the HP EFS WAN Accelerators. You can enable failover support in the Management Console or you can use the HP EFS WAN Accelerator command-line interface (CLI).

---

## Bypass Mode

The HP EFS WAN Accelerator is equipped with one of the following types of bypass interfaces (depending on your order):

- ◆ HP EFS N2c WAN Accelerator 2-port NIC Card
- ◆ HP EFS N4c WAN Accelerator 4-port NIC Card
- ◆ HP EFS N2f WAN Accelerator 2-port NIC Card

For detailed information about bypass card status lights, see the *HP StorageWorks Enterprise File Services WAN Accelerator Bypass NIC Installation Guide*.

If there is a serious problem with the HP EFS WAN Accelerator or it is not powered on, it goes into bypass mode to prevent a single point of failure. If the HP EFS WAN Accelerator is in bypass mode, you are notified in the following ways:

- ◆ The Intercept/Bypass status light is active. For detailed information about the status lights for each of the bypass cards, see the *HP StorageWorks Enterprise File Services WAN Accelerator Bypass NIC Installation Guide*.
- ◆ **Critical** is displayed in the status bar of the Management Console.
- ◆ Simple Network Management Protocol (SNMP) traps are sent (if you have set this option).
- ◆ The event is logged to system logs (**syslog**) (if you have set this option).
- ◆ Email notifications are sent (if you have set this option).

In an HP EFS WAN Accelerator in-path configuration, in the case of a failure, the appliance automatically switches to bypass mode. Traffic that was passed-through is uninterrupted. Traffic that was optimized might be interrupted, depending on the behavior of the application-layer protocols. When connections are restored, they succeed, although without optimization.

When the fault is corrected, new connections that are made receive optimization; however, connections made during the fault are not. To force all connections to be optimized, enable the *kickoff* feature. Generally, connections are short lived and kickoff is not necessary. For detailed information about enabling the kickoff feature, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

---

**TIP:** You can close old connections in the Reports: Current Connections page of the Management Console. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

---

In an out-of-path deployment, if the HP EFS WAN Accelerator fails, the first connection from the client fails. After detecting that the HP EFS WAN Accelerator is down, an **HP EFS WAN Accelerator-ping** channel is setup from the client-side HP EFS WAN Accelerator to the server-side HP EFS WAN Accelerator. Subsequent connections are passed through unoptimized. When the **HP EFS WAN Accelerator-ping** succeeds, processing is restored and subsequent connections are intercepted and optimized. For detailed information about the **HP EFS WAN Accelerator-ping** command, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual*.

---

## Failover Mode

You can deploy redundant HP EFS WAN Accelerators in your network to ensure optimization continues if there is a failure in one of the HP EFS WAN Accelerators. If the HP EFS WAN Accelerator is in failover mode:

- ◆ optimization is lost on the current connections on the master HP EFS WAN Accelerator.
- ◆ the backup HP EFS WAN Accelerator takes over and all new connections are optimized.
- ◆ when the master HP EFS WAN Accelerator comes back up, the backup HP EFS WAN Accelerator stops optimizing connections.



**CHAPTER 2**

# In-Path Deployments

## In This Chapter

This chapter describes physical in-path network deployments and summarizes the basic steps for configuring them. This chapter includes the following sections:

- ◆ “[Introduction to Physical In-Path Deployments](#),” next
- ◆ “[In-Path, Failover Support Deployment](#)” on page 18
- ◆ “[In-Path, Two Routing Points Deployment](#)” on page 20
- ◆ “[In-Path, Server-Side Deployment](#)” on page 21
- ◆ “[In-Path, Server-Side, One to One Deployment](#)” on page 22

This chapter assumes that you are familiar with the HP EFS WAN Accelerator Management Console (Management Console). For detailed information about the Management Console and how to use it, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

This chapter also assumes that you are familiar with the installation and configuration process for the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

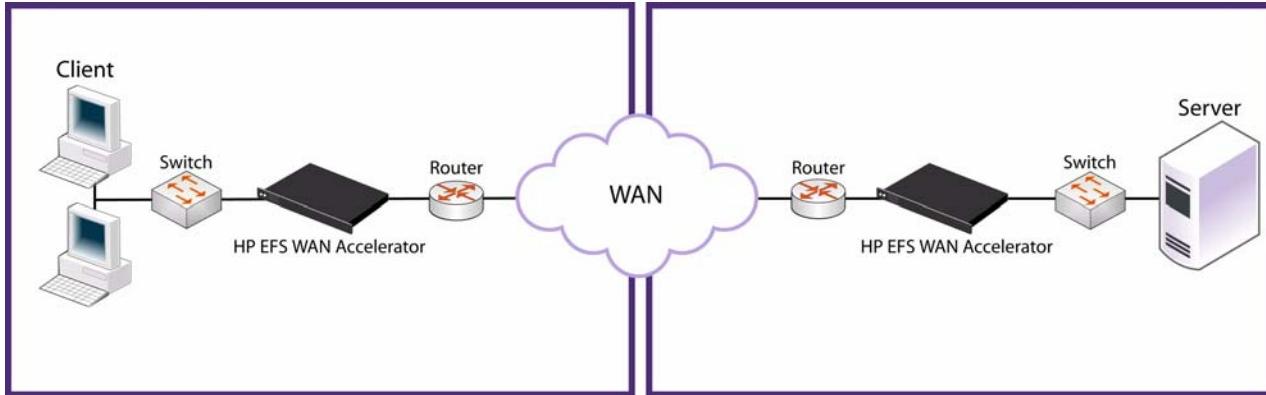
This chapter provides the basic steps for physical in-path network deployments. It does not provide detailed procedures. Use this chapter as a general guide for these deployments. If you need additional assistance, contact HP technical support at <http://www.hp.com>.

For detailed information about the factors you must consider before you deploy the HP EFS WAN Accelerator, see “[Design and Deployment Overview](#)” on page 11.

## Introduction to Physical In-Path Deployments

The following section describes physical in-path network configurations where the HP EFS WAN Accelerator is physically in the direct path between clients and servers. The clients and servers continue to see client and server Internet Protocol (IP) addresses. Physical in-path configurations are suitable for locations where the total bandwidth is within the limits of the installed HP EFS WAN Accelerator.

**Figure 2-1.** Physically In-Path, Client and Server-Side Deployment

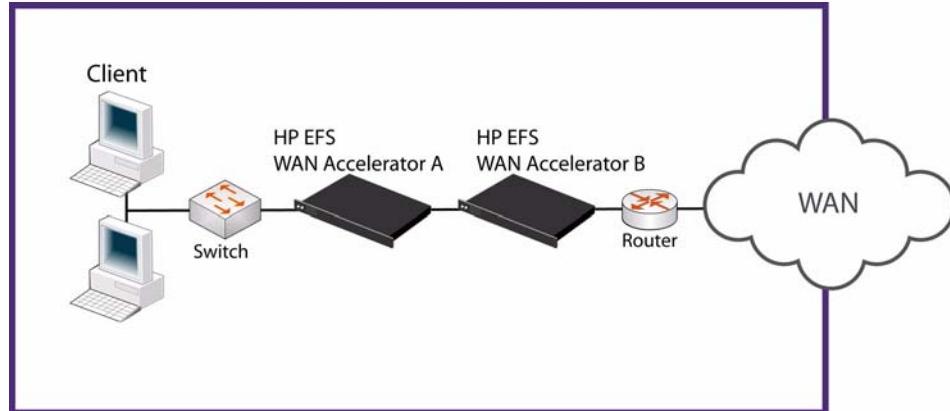


## In-Path, Failover Support Deployment

An in-path, fail-over support deployment serves offices with one WAN routing point and where network disruptions are unacceptable. This deployment is cost effective, simple to manage, and continues to optimize data if there is an error in the system.

The following figure illustrates the client-side of the network where redundant HP EFS WAN Accelerators are deployed to provide optimization of data.

**Figure 2-2.** In-Path, Failover Deployment



### Basic Steps (Client-Side)

Perform the following steps for each client-side HP EFS WAN Accelerator.

1. Configure the HP EFS WAN Accelerator as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
3. Navigate to the Setup: Advanced Networking - Failover Settings page in the Management Console.
4. Enable failover support. For example:
  - ◆ On HP EFS WAN Accelerator A: specify HP EFS WAN Accelerator A as the *master* and specify the in-path IP address of HP EFS WAN Accelerator B as the *backup* (other) IP address.
  - ◆ On HP EFS WAN Accelerator B: specify HP EFS WAN Accelerator B as the *backup* (other) and specify the in-path IP address of HP EFS WAN Accelerator A as the *master* IP address.

**Figure 2-3.** Setup: Advanced Networking - Failover Settings Page

The screenshot shows the 'Advanced Networking - Failover Settings' page. At the top, there is a navigation bar with links for Home, Setup, Reports, Logging, Help, and a status indicator 'Status: Healthy'. To the right of the status is a 'Logged in as: admin [logout]' link. Below the navigation bar is a sidebar with a dark background containing a list of management options. The 'Advanced Networking' section is expanded, showing 'Failover Settings' as the selected item. The main content area has two main sections: 'Failover Settings' and 'Automated Online Datastore Settings'. Under 'Failover Settings', there is a checked checkbox for 'Enable Failover Support'. Below it, a dropdown menu labeled 'Current Appliance is the:' is set to 'Master'. Another dropdown menu labeled 'Other Appliance's Inpath IP Address' has 'Master' and 'Backup' listed. Under 'Automated Online Datastore Settings', there is an unchecked checkbox for 'Enable Automated Online Datastore Synchronization'. Below it, a dropdown menu labeled 'Current Appliance is the:' is set to 'Master'. There are also input fields for 'Synchronization Port' (set to '0'), 'Reconnection interval' (set to '30 secs'), and 'Other Appliance's IP Address' (set to '10.0.0.3'). At the bottom right of the page are three buttons: 'Apply', 'Save', and 'Reset'.

5. Enable Automated Online Datastore Synchronization. For example:
  - ◆ Select Master or Backup from the **Current Appliance is the** drop-down list.
  - ◆ Type a port number in the **Synchronization Port** text box. The default value is 7744.

- ◆ Type the number of seconds in the **Reconnection interval** text box. The default value is 30.
6. Type the backup HP EFS WAN Accelerator's IP address in the **Other Appliance's In-path IP Address** text box.
  7. Apply and save the new configuration in the Management Console.
  8. Begin optimization. View performance reports and system logs in the Management Console.

## Basic Steps (Server-Side)

The server-side HP EFS WAN Accelerator is configured as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

---

## In-Path, Two Routing Points Deployment

An in-path, two routing point deployment serves offices with two WAN routing points and redundant HP EFS WAN Accelerators. This deployment is simple to manage, provides failover support, and load balances traffic.

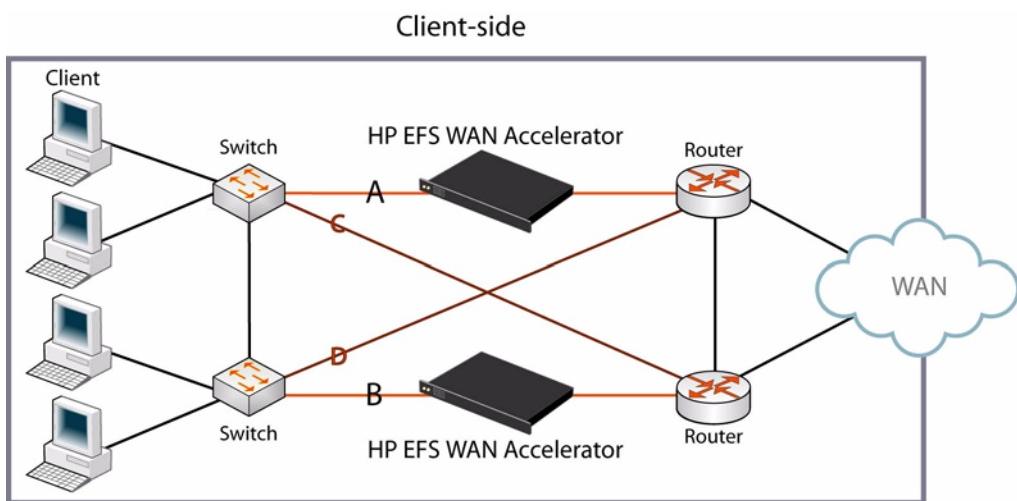
For an in-path, two routing point deployment you must configure the Interior Gateway Protocol (IGP) to prefer HP EFS WAN Accelerator links (links A, B in the figure below) over non-HP EFS WAN Accelerator links for load balancing to occur. For any given flow, under all conditions, both halves of the connection will use the same link (A, B).

---

**IMPORTANT:** HP strongly recommends that you use an HP EFS N4c WAN Accelerator 4-port NIC Card or connection forwarding for an in-path, two routing points deployment. For detailed information about connection forwarding, see [Chapter 5, “Configuring Connection Forwarding.”](#)

---

The following figure illustrates the client-side of the network where two in-path HP EFS WAN Accelerators are configured as in-path interfaces.

**Figure 2-4.** In-Path, Two Routing Points Deployment

## Basic Steps (Client-Side)

Perform the following steps on each client-side HP EFS WAN Accelerator.

1. Configure the HP EFS WAN Accelerator as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console to verify your configuration. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
3. Configure your Interior Gateway Protocol (IGP) to prefer links A and B over links C and D.
4. Apply and save the new configuration in the Management Console.
5. Begin optimization. View performance reports and system logs in the Management Console.

## Basic Steps (Server-Side)

The server-side HP EFS WAN Accelerator is configured as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

---

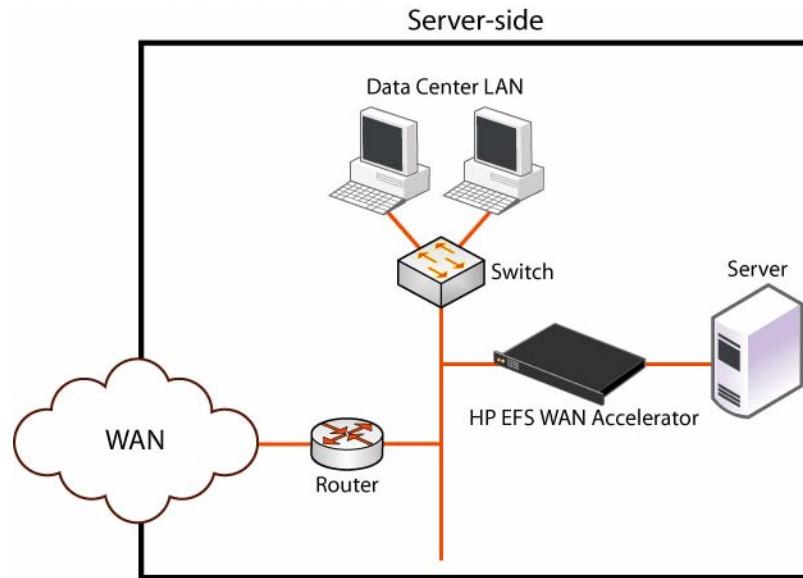
## In-Path, Server-Side Deployment

An in-path, server-side deployment serves a single server or server subnet. This deployment is simple to manage and LAN traffic is passed-through unoptimized. It does not provide failover support if there is an error in the system.

This deployment is useful in environments where most of the server-side traffic is out-of-path but there are applications that originate on the server-side that require optimization (for example, backup software, software distribution suites, or other similar applications).

The following figure illustrates a server-side subnet where the HP EFS WAN Accelerator is deployed to provide data center clients with optimized data.

**Figure 2-5. In-Path, Server-Side Deployment**



## **Basic Steps (Client-Side)**

The client-side HP EFS WAN Accelerator is configured as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

## **Basic Steps (Server-Side)**

The server-side HP EFS WAN Accelerator is configured as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

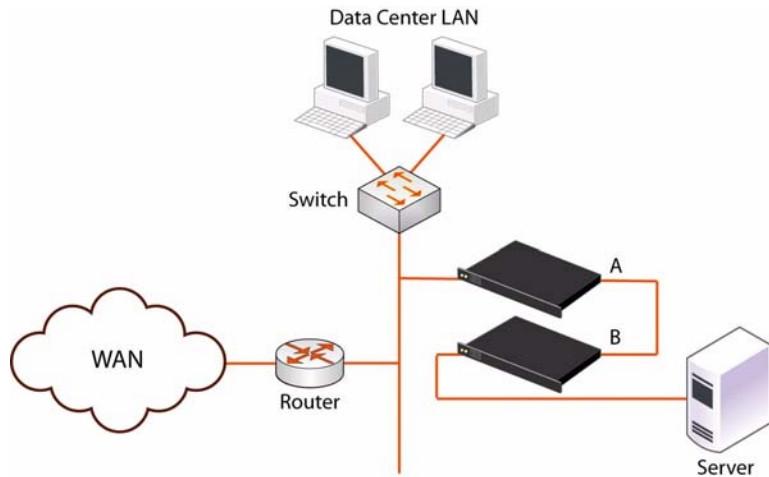
---

## **In-Path, Server-Side, One to One Deployment**

An in-path, server-side, One to One deployment is appropriate for data center LANs where you want to optimize applications on a single server or server subnet. This deployment is simple to manage and LAN traffic is passed-through.

The following figure illustrates the server-side of the network.

**Figure 2-6. In-Path, Server-Side, One to One Deployment**



## Basic Steps (Client-Side)

The client-side HP EFS WAN Accelerator is configured as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

## Basic Steps (Server-Side)

Perform the following steps for each of the server-side HP EFS WAN Accelerators.

1. Configure the HP EFS WAN Accelerator as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
3. Navigate to the Setup: Advanced Networking - Failover Settings page in the Management Console.
4. Enable failover support. For example:
  - ◆ On HP EFS WAN Accelerator A, specify HP EFS WAN Accelerator A as the *master* and specify the in-path IP address of HP EFS WAN Accelerator B as the *backup (other)* IP address.

- ◆ On HP EFS WAN Accelerator B, specify HP EFS WAN Accelerator B as the *backup* (other) and specify the in-path IP address of HP EFS WAN Accelerator A as the *master* IP address.

**Figure 2-7.** Setup: Advanced Networking - Failover Settings Page

The screenshot shows the 'Advanced Networking - Failover Settings' page. The left sidebar has a tree view with 'Advanced Networking' expanded, showing 'Failover Settings' selected. The main area has a heading 'Failover Settings' with a note: 'Check and modify your failover configuration. This page is optional.' It contains two sections: 'Failover Support' (checkbox checked, dropdown 'Current Appliance is the:' set to 'Master') and 'Automated Online Datastore Settings' (checkbox unchecked, dropdown 'Current Appliance is the:' set to 'Master', input 'Synchronization Port' set to '0', input 'Reconnection interval' set to '30 secs', input 'Other Appliance's IP Address' set to '10.0.0.3'). At the bottom are 'Apply', 'Save', and 'Reset' buttons.

- Under Automated Online Datastore Settings, click **Enable Automated Online Datastore Synchronization**.
  - Select Master or Backup from the **Current Appliance is the** drop-down list.
  - Type a port number in the **Synchronization Port** text box. The default value is 7744.
  - Type the number of seconds in the **Reconnection interval** text box. The default value is 30.
- Type the backup HP EFS WAN Accelerator's IP address in the **Other Appliance's In-path IP Address** text box.
- Apply and save the new configuration in the Management Console.
- Begin optimization. View performance reports and system logs in the Management Console.

## CHAPTER 3

# Virtual In-Path Network Deployments

## In This Chapter

This chapter describes virtual in-path deployments and summarizes the basic steps for configuring them. This chapter includes the following sections:

- ◆ “[Introduction to Virtual In-Path Deployments](#),” next
- ◆ “[In-Path, Load Balanced, Layer-4 Switch](#)” on page 26

This chapter assumes you are familiar with the HP EFS WAN Accelerator Management Console (Management Console). For detailed information about the Management Console and how to use it, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

This chapter also assumes that you are familiar with the installation and configuration process for the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

This chapter provides the basic steps for virtual in-path deployments. It does not provide detailed procedures. Use this chapter as a general guide to these deployments. If you need additional assistance, contact HP technical support located at <http://www.hp.com>.

For detailed information about the factors you must consider before you design and deploy the HP EFS WAN Accelerator in a network environment, see “[Design and Deployment Overview](#)” on page 11.

---

## Introduction to Virtual In-Path Deployments

In a virtual in-path deployment, the HP EFS WAN Accelerator is virtually in the path between clients and servers. In a virtual in-path deployment, clients and servers continue to see client and server IP addresses. This deployment differs from a physical in-path deployment in that a packet redirection mechanism is used to direct packets to HP EFS WAN Accelerators that are not in the physical path of the client or server. Redirection mechanisms include:

- ◆ **Layer-4 Switch.** You enable Layer 4 switch (or server load-balancers) support when you have multiple HP EFS WAN Accelerators in your network to manage large bandwidth requirements.
- ◆ **Hybrid.** A hybrid deployment is a deployment in which the HP EFS WAN Accelerator is both in-path and out-of-path. A hybrid deployment is useful where the HP EFS WAN Accelerator must be referenced from remote sites as an out-of-path device (for example, to avoid mistaken auto-discovery or to bypass intermediary HP EFS WAN Accelerators). For detailed information, see [Chapter 4, “Out-of-Path Network Deployments.”](#)
- ◆ **WCCP.** WCCP was originally implemented on Cisco routers, multi-layer switches, and Web caches to redirect HTTP requests to local Web caches (Version 1). Version 2, which is implemented on HP EFS WAN Accelerators, can redirect any type of connection from multiple routers or Web caches. For example, if you have multiple routers or it there is not a virtual place for the HP EFS WAN Accelerator, you can place the HP EFS WAN Accelerator to be virtually in-path through the router so that they work together. Typically, you configure WCCP on the client-side HP EFS WAN Accelerator. For detailed information, see [Chapter 7, “WCCP Deployments.”](#)
- ◆ **Policy-Based Routing (PBR).** PBR enables you to redirect traffic to an HP EFS WAN Accelerator that is configured as an out-of-path device. PBR allows you to define policies to route packets instead of relying on routing protocols. You define policies to redirect traffic to the HP EFS WAN Accelerator and policies to avoid loop-back. For detailed information, see [Chapter 6, “Policy-Based Routing Deployments.”](#)

## In-Path, Load Balanced, Layer-4 Switch

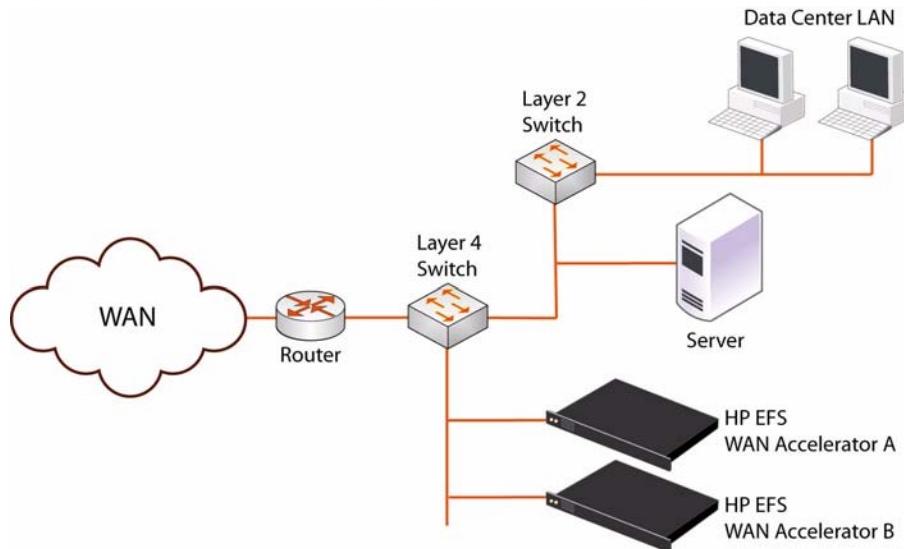
An in-path, load-balanced, Layer-4 switch deployment serves high traffic environments or environments with large numbers of active Transmission Control Protocol (TCP) connections. It handles failures, scales easily, and supports all protocols.

When you configure the HP EFS WAN Accelerator using a Layer-4 switch, you define the HP EFS WAN Accelerators as a pool where the Layer-4 switch redirects client and server traffic.

Only one WAN interface on the HP EFS WAN Accelerator is connected to the Layer-4 switch and the HP EFS WAN Accelerator is configured to send and receive data through that interface.

The following figure illustrates the server-side of the network where load balancing is required.

**Figure 3-1.** In-Path, Load-Balanced, Layer-4 Switch Deployment



## Basic Steps (Client-Side)

The client-side HP EFS WAN Accelerator is configured as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

## Basic Steps (Server-Side)

Perform the following steps for each HP EFS WAN Accelerator in the cluster.

1. Mount and power on the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*. Make sure you properly connect to the Layer-2 switch. For example:
  - ◆ On HP EFS WAN Accelerator A, plug the straight-through cable into the Primary port of the HP EFS WAN Accelerator and connect it to the LAN port of the Layer-2 switch.
  - ◆ On HP EFS WAN Accelerator B, plug the straight-through cable into the Primary port of the HP EFS WAN Accelerator and connect it to the LAN port of the Layer-2 switch.
3. Configure the HP EFS WAN Accelerator in an in-path configuration. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
4. Connect the Layer-4 switch to the HP EFS WAN Accelerator:
  - ◆ On HP EFS WAN Accelerator A, plug the straight-through cable into the WAN port of the HP EFS WAN Accelerator and the Layer-4 switch.

- ◆ On HP EFS WAN Accelerator B, plug the straight-through cable into the WAN port of the HP EFS WAN Accelerator and the Layer-4 switch.
5. Connect to the Management Console. For details see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
  6. Navigate to the Setup: Optimization Service - General Settings page in the Management Console.
  7. Enable Layer-4 switch support. For example:
    - ◆ Click **Enable In-Path Support** and **Enable L4/PBR/WCCP Support on Interface wan0\_0**.

**Figure 3-2.** Setup: Optimization Service - General Settings Page

The screenshot shows the 'Optimization Service - General Settings' page. The left sidebar has a tree view with 'General Settings' expanded. The main area shows the 'In-Path' configuration with several checkboxes. The 'Out-of-Path' section is collapsed. At the bottom are 'Apply', 'Save', and 'Reset' buttons.

8. Apply and save the new configuration in the Management Console.
9. Configure your L4 switch.
10. Restart the HP EFS WAN Accelerator in the Setup: Start/Stop Appliance page of the Management Console.
11. Begin optimization. View performance reports and system logs in the Management Console.

## CHAPTER 4

# Out-of-Path Network Deployments

## In This Chapter

This chapter describes out-of-path deployments and summarizes the basic steps for configuring them. This chapter includes the following sections:

- ◆ “[Introduction to Out-of-Path Deployments](#),” next
- ◆ “[Out-of-Path, Failover Deployment](#)” on page 30
- ◆ “[Out-of-Path, Static Cluster Deployment](#)” on page 33
- ◆ “[Hybrid: In-Path and Out-of-Path Deployment](#)” on page 35

This chapter assumes you are familiar with the HP EFS WAN Accelerator Management Console (Management Console). For detailed information about the Management Console and how to use it, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

This chapter also assumes that you are familiar with the installation and configuration process for the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

This chapter provides the basic steps for out-of-path network deployments. It does not provide detailed procedures. Use this chapter as a general guide to these deployments. If you need additional assistance, contact HP technical support located at <http://www.hp.com>.

For detailed information about the factors you must consider before you design and deploy the HP EFS WAN Accelerator in a network environment, see “[Design and Deployment Overview](#)” on page 11.

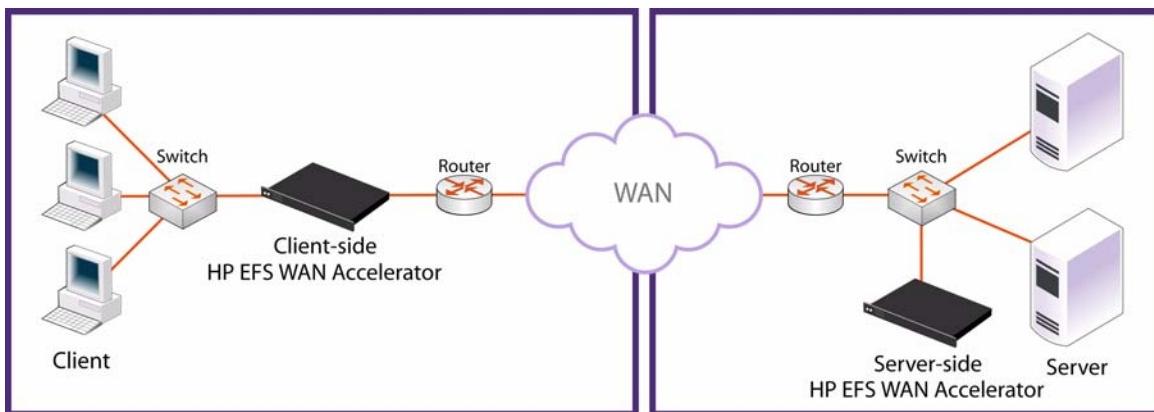
---

## Introduction to Out-of-Path Deployments

An out-of-path deployment is a network configuration in which the HP EFS WAN Accelerator is not in the direct physical path between the client and the server. In an out-of-path deployment, the HP EFS WAN Accelerator acts as a proxy. An out-of-path configuration is suitable for data center locations where physical in-path or virtual in-path configurations are not possible.

Typically, in an out-of-path deployment, the client-side HP EFS WAN Accelerator is configured as an in-path device, and the server-side HP EFS WAN Accelerator is configured as an out-of-path device.

**Figure 4-1. Physical Out-of-Path Deployment**



---

## Out-of-Path, Failover Deployment

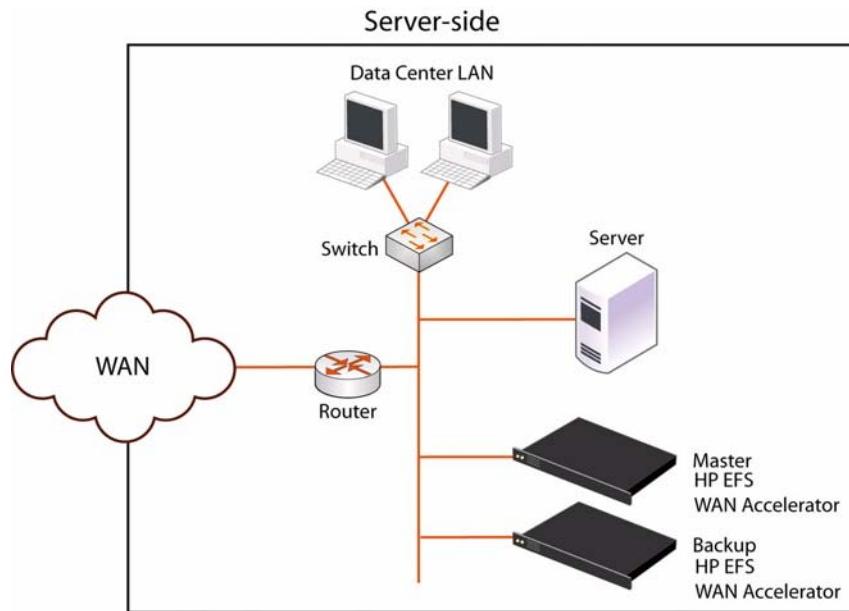
An out-of-path, failover deployment serves networks where an in-path deployment is not an option. This deployment is cost effective, simple to manage, and provides redundancy.

In an out-of-path, failover deployment, two HP EFS WAN Accelerators are deployed. When both HP EFS WAN Accelerators are functioning properly, the connections traverse the master appliance. If the master HP EFS WAN Accelerator fails, subsequent connections traverse the backup HP EFS WAN Accelerator.

When the master HP EFS WAN Accelerator is restored, the next connection traverses the master HP EFS WAN Accelerator. If both HP EFS WAN Accelerators fail, the connection is passed through unoptimized to the server.

The following figure illustrates the server-side of the network where two HP EFS WAN Accelerators are deployed in an out-of-path configuration to ensure that data continues to be optimized if there is an error in the system.

**Figure 4-2.** Out-of-Path, Server-Side, Failover Support Deployment



## Basic Steps (Client-Side)

In an out-of-path, two HP EFS WAN Accelerator failover deployment, the client-side HP EFS WAN Accelerator is configured as an in-path device with fixed-target rules that point to the server-side, out-of-path HP EFS WAN Accelerators.

1. Configure the HP EFS WAN Accelerator as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
3. Navigate to the Setup: Optimization Service - In-Path Rules page in the Management Console.

**Figure 4-3.** Setup: Optimization Service - In-Path Rules Page

The screenshot shows the 'Optimization Service - In-Path Rules' page. The left sidebar contains a navigation menu with sections like Optimization Service, Host Settings, Advanced Networking, and Configuration Manager. The main area has a header 'Optimization Service - In-Path Rules' with a note: 'Check and modify your in-path rules. By default, all traffic going through this appliance is optimized.' Below is a table of rules:

#	Type	Source	Destination	Port	Target	Port	Opt Policy	Neural	VLAN
1	Pass	All	All	Secure	--	--	--	--	All
2	Pass	All	All	Interactive	--	--	--	--	All
def	Auto	All	All	All	--	--	Normal	Always	All

Buttons at the bottom include 'Remove Selected Rules', 'Move Rule', and 'Move Rule' dropdowns. An 'Add New Rule' section follows:

**Add New Rule:**

- Type: Fixed-Target
- Insert Rule At: end
- Source Subnet: 0.0.0.0/0
- Destination Subnet: 0.0.0.0/0
- Port: all
- Targets:

  - Target Appliance IP: 10.0.0.4 Port: 7810
  - Backup Appliance IP: 10.0.0.3 Port: 7810

- Advanced Options (click to open):
  - VLAN Tag ID: All
  - Optimization Policy: Normal
  - Neural Framing Mode: Always

Buttons: Add Rule, Save, Reset.

4. To enable failover support for the out-of-path HP EFS WAN Accelerators, define a fixed-target rule that points to the main and backup targets. For example:
  - ◆ Type the out-of-path, server-side HP EFS WAN Accelerator IP address and port in the **Target Appliance IP** and **Port** text boxes.

- ◆ Type the backup HP EFS WAN Accelerator IP address and port in the **Backup Appliance IP** and **Port** text boxes.

5. Save and apply the new configuration in the Management Console.

6. Begin optimization. View performance reports and system logs in the Management Console.

## Basic Steps (Server-Side)

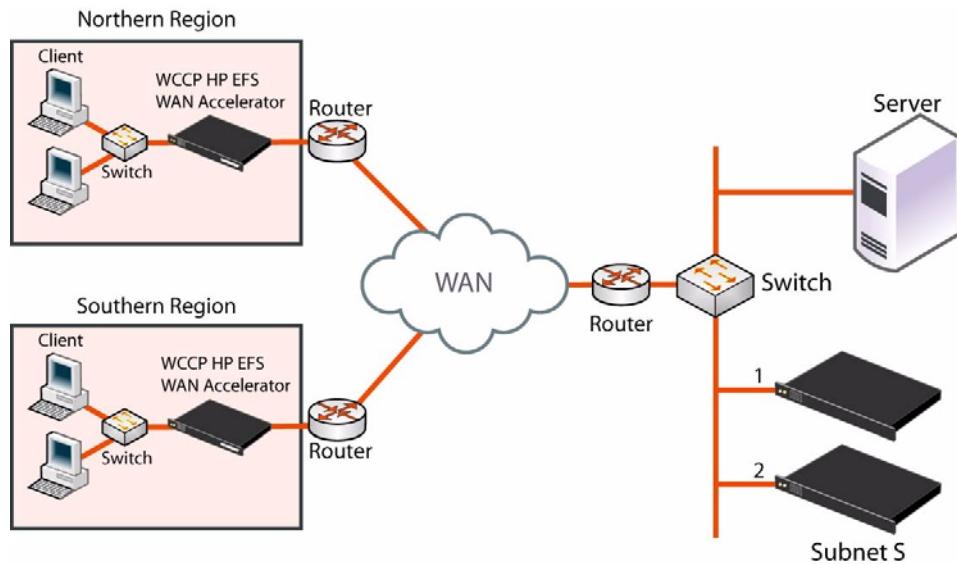
The server-side HP EFS WAN Accelerators are configured as out-of-path devices. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

## Out-of-Path, Static Cluster Deployment

An out-of-path, static cluster deployment is appropriate when an in-path deployment is not an option. This deployment handles failures and scales to very high traffic levels.

The following figure illustrates a deployment where two HP EFS WAN Accelerators are configured as out-of-path devices on the server-side of the network and there are static clusters with in-path HP EFS WAN Accelerators on the client-side of the network.

**Figure 4-4. Static Cluster Deployment**



## Basic Steps (Client-Side)

Perform the following steps for each HP EFS WAN Accelerator on the client-side of the network.

1. Configure the HP EFS WAN Accelerators as in-path devices. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
3. Navigate to the Setup: Optimization Service - In-Path Rules page in the Management Console.
4. Define fixed-target rules for the set of HP EFS WAN Accelerators in each cluster of user sites. For example:
  - ◆ In the Northern region, for all the HP EFS WAN Accelerators in the set, define HP EFS WAN Accelerator 1 as the fixed target for servers in Subnet S.
  - ◆ In the Southern region, for all HP EFS WAN Accelerators in the set, define HP EFS WAN Accelerator 2 as the fixed target for servers in Subnet S.

**Figure 4-5.** Setup: Optimization Service - In-Path Rules, Fixed Target Page

#	Type	Source	Destination	Port	Target	Port	Opt Policy	Neural	VLAN
1	Fixed	All	All	All	10.0.0.3 10.0.0.2	135 135	Normal	Always	All
def	Auto	All	All	All	--	--	Normal	Always	All

5. Apply and save the new configuration in the Management Console.

6. Begin optimization. View performance reports and system logs in the Management Console.

## Basic Steps (Server-Side)

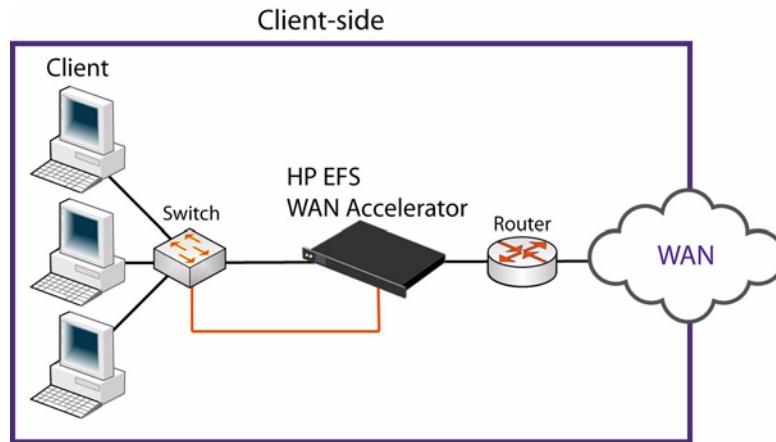
For the server-side, HP EFS WAN Accelerators, follow the procedures for an out-of-path, failover support deployment. For detailed information, see “[Out-of-Path, Failover Deployment](#)” on page 30.

## Hybrid: In-Path and Out-of-Path Deployment

A hybrid deployment serves offices with one WAN routing point and users, and where the HP EFS WAN Accelerator must be referenced from remote sites as an out-of-path device (for example, to avoid mistaken auto-discovery or to bypass intermediary HP EFS WAN Accelerators).

The following figure illustrates the client-side of the network where the HP EFS WAN Accelerator is configured as both an in-path and out-of-path device.

**Figure 4-6.** Hybrid: In-Path and Out-of-Path Deployment



## Basic Steps (Client-Side)

Perform the following steps for the HP EFS WAN Accelerator.

1. Configure the HP EFS WAN Accelerator as an in-path and out-of-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console to verify your configuration. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
3. Navigate to the Setup: Optimization Service - In-Path Rules page in the Management Console.

**Figure 4-7. Setup: Optimization Service - In-Path Rules Page**

The screenshot shows the 'Optimization Service - In-Path Rules' page. The left sidebar contains navigation links for Optimization Service (General Settings, In-Path Rules, Protocols), Host Settings, Advanced Networking, Port Labels, Reports, Logging, Date & Time, Authentication, Licenses, Scheduled Jobs, Configuration Manager, and Upgrade Software. The main content area has a title 'Optimization Service - In-Path Rules' with a note: 'Check and modify your in-path rules. By default, all traffic going through this appliance is optimized.' Below is a table of existing rules:

#	Type	Source	Destination	Port	Target	Port	Opt Policy	Neural	VLAN
1	Pass	All	All	Secure	--	--	--	--	All
2	Pass	All	All	Interactive	--	--	--	--	All
def	Auto	All	All	All	--	--	Normal	Always	All

Buttons include 'Remove Selected Rules', 'Move Rule' (with dropdowns for rule number and position), and 'Move Rule' button. A large 'Add New Rule:' section is open, containing fields for Type (Fixed-Target selected), Insert Rule At (end selected), Source Subnet (0.0.0.0/0), Destination Subnet (0.0.0.0/0), Port (all), Targets (Target Appliance IP: 10.0.0.4, Port: 7810; Backup Appliance IP: 10.0.0.3, Port: 7810), Advanced Options (VLAN Tag ID: All, Optimization Policy: Normal, Neural Framing Mode: Always), and an 'Add Rule' button. Below is an 'Additional Options:' section with a checkbox for 'Enable Computation of Neural Heuristics' and an 'Update Settings' button. At the bottom are 'Save' and 'Reset' buttons.

4. Define in-path, fixed-target rules for traffic you want to optimize. For example:
  - ◆ Select **start**, **end**, or a **rule number** from the **Insert Rule At** drop-down list to insert a rule in the Rules list. When you specify a particular rule number, the rule is placed after the rule number you specified and before the default auto-discover rule.
  - ◆ Type the IP address for the source subnet in the **Source Subnet** text box. Use the following format: **0.0.0.0/0**.

- ◆ Type the IP address and port for the destination subnet, in the **Destination Subnet** and **Port** text boxes. To specify all ports, type **all** in the Port text box.
- ◆ Under Targets, type the IP address and port number for the HP EFS WAN Accelerator that is the peer in the **Target Appliance IP** and **Port** text boxes. The IP address must be the Primary Port IP address on the target HP EFS WAN Accelerator. The default port is **7810**.
- ◆ If you have a backup, out-of-path HP EFS WAN Accelerator in your system (failover support), type the IP address and port for the backup appliance in the **Backup Appliance IP** and **Port** text boxes. Use the following format: **0.0.0.0/0**. The default port is **7810**.

5. Apply and save the new configuration in the Management Console.
6. Begin optimization. View performance reports and system logs in the Management Console.

## Basic Steps (Server-Side)

The server-side HP EFS WAN Accelerator is configured as an out-of-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

1. Navigate to the Setup: Optimization Service - General Settings page in the Management Console.

2. Enable out-of path support click **Enable Out-of-Path Support**.

**Figure 4-8.** Setup: Optimization Service - General Settings Page

The screenshot shows the 'Optimization Service - General Settings' page. The left sidebar has a dark background with white text, listing various service options like Optimization Service, Configuration Manager, and Upgrade Software. The main content area has a light gray background. At the top, there's a navigation bar with links for Home, Setup, Reports, Logging, Help, and a status indicator 'Status: Healthy'. To the right of the status is 'Logged in as: admin [logout]'. Below the status, there's a section titled 'Optimization Service - General Settings' with a sub-section 'In-Path'. Under 'In-Path', there's a checkbox for 'Enable In-Path Support' with two sub-options: 'Reset Existing Client Connections on Start Up' and 'Enable L4/PBR/WCCP Support on Interface wan0\_0'. Below this is a section titled 'Out-of-Path (for server-side appliances only)' containing a checked checkbox for 'Enable Out-of-Path Support'. At the bottom right of the page are three buttons: 'Apply', 'Save', and 'Reset'.



## CHAPTER 5

# Configuring Connection Forwarding

## In This Chapter

This chapter describes how to deploy the HP EFS WAN Accelerator in asymmetric server-side networks using connection forwarding. This chapter includes the following sections:

- ◆ “Introduction to Connection Forwarding,” next
- ◆ “One-to-One Failover Deployment” on page 41
- ◆ “Configuring Connection Forwarding” on page 41

This chapter assumes you are familiar with the HP EFS WAN Accelerator Management Console (Management Console). For detailed information about the Management Console and how to use it, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

This chapter also assumes that you are familiar with the installation and configuration process for the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

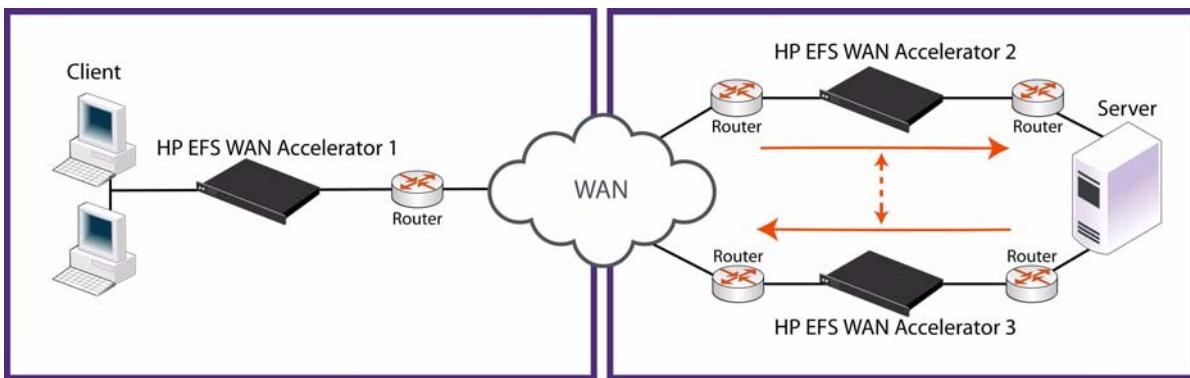
---

## Introduction to Connection Forwarding

In asymmetric networks, a client request traverses a different network path than the server response. Although the packets traverse different paths, to optimize a connection, packets traveling in both directions must pass through the same client-side and server-side HP EFS WAN Accelerator.

If you have one path (through HP EFS WAN Accelerator-2) from the client to the server and a different path (through HP EFS WAN Accelerator-3) from the server to the client, you need to enable in-path connection forwarding and configure the HP EFS WAN Accelerators to communicate with each other. These HP EFS WAN Accelerators are called *neighbors* and exchange connection information to redirect packets to each other.

**Figure 5-1.** Connection Forwarding in an Asymmetric Network



For example, in [Figure 5-1](#) packets from the Client to the Server go through HP EFS WAN Accelerator-2 while packets from the server to the Client go through HP EFS WAN Accelerator-3. The connection is intercepted by HP EFS WAN Accelerator-1 and HP EFS WAN Accelerator-2 because the first Transmission Control Protocol (TCP) packet went through HP EFS WAN Accelerator-2.

Because HP EFS WAN Accelerator-3 sees the packets but HP EFS WAN Accelerator-2 has the relevant information to optimize them, HP EFS WAN Accelerator-3 redirects the packets from the Server to the Client back to HP EFS WAN Accelerator-2 so that the connection can be intercepted and optimized correctly by HP EFS WAN Accelerator-2.

## Neighbors in Connection Forwarding

Neighbors can be placed in the same physical site or in different sites but the latency between them should be small because the packets travelling between them are not optimized.

**TIP:** If the neighbors are placed on the same physical site, consider installing and configuring an HP EFS WAN Accelerator with multiple pairs of ports (for example, HP EFS N4c WAN Accelerator 4-port NIC Card) and connecting the multiple links to intercept all packets coming back from the server without performing connection forwarding.

## Load-Balancing

Connection forwarding can also be used in networks where there is packet load-balancing on the server-side, because it does not matter which path the packets take when they come back from the server. Connection forwarding cannot perform packet load-balancing on the client-side (that is, there is no redirection on the client-side).

If there are more than two possible paths, additional HP EFS WAN Accelerators must be installed on each path and configured as neighbors. Neighbors receive information in parallel (the delay introduced at connection set up is equal to the time it takes to get an acknowledgement from the furthest neighbor).

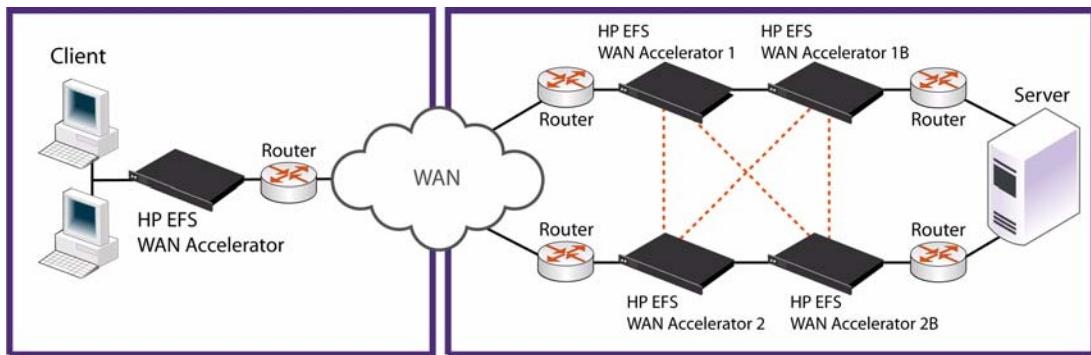
If one of the neighbor HP EFS WAN Accelerators reaches its optimization capacity limit, that HP EFS WAN Accelerator will not accept new connections, but it redirects packets to other neighbors for optimization.

## One-to-One Failover Deployment

To ensure optimization in the event of a failure, a backup HP EFS WAN Accelerator can be added to each neighbor HP EFS WAN Accelerator in a one-to-one failover configuration.

In [Figure 5-2](#) there are two HP EFS WAN Accelerators on each path that are configured in a one-to-one failover mode. Each HP EFS WAN Accelerator must be a neighbor of the master and backup HP EFS WAN Accelerators on the other paths.

**Figure 5-2.** One-to-One Failover Deployment



HP EFS WAN Accelerator-2 and HP EFS WAN Accelerator-2B are configured as neighbors of HP EFS WAN Accelerator-1 which exchanges connection information with both of them so that if either HP EFS WAN Accelerator-2 or HP EFS WAN Accelerator-2B fails, the other redirects packets to HP EFS WAN Accelerator-1.

In [Figure 5-2](#), packets from the server are redirected by HP EFS WAN Accelerator-2B unless it fails in which case they are redirected by HP EFS WAN Accelerator-2.

As long as one of the two failover HP EFS WAN Accelerators on each path is up, connections are intercepted. If the two HP EFS WAN Accelerators on the same path fail, connections stop being intercepted and optimized.

## Configuring Connection Forwarding

The following section describes the basic steps for configuring connection forwarding.

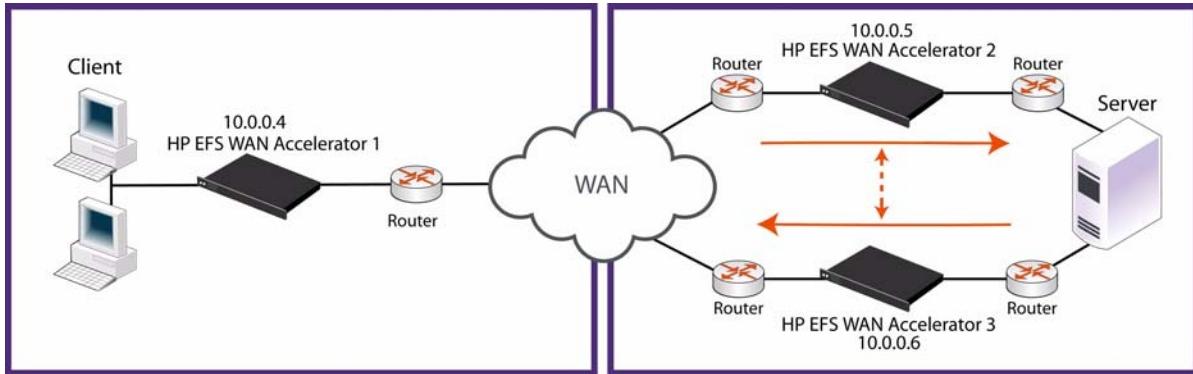
You can configure connection forwarding using the Management Console or the HP EFS WAN Accelerator command-line interface (CLI).

## Configuring Connection Forwarding Using the Management Console

The following section describes the basic steps for enabling and configuring connection forwarding using the Management Console.

The following figure illustrates a network deployment in which the packets from the client to the server go through HP EFS WAN Accelerator-2 while packets from the server to the client go through HP EFS WAN Accelerator-3. From HP EFS WAN Accelerator-3 the packets are sent to HP EFS WAN Accelerator-2, through the virtual path.

**Figure 5-3. Connection Forwarding in an Asymmetric Network**



**IMPORTANT:** When you define a neighbor, you must specify the HP EFS WAN Accelerator in-path IP address, not the primary IP address.

### Basic Steps (Client-Side)

Perform the following step on each of the client-side HP EFS WAN Accelerators.

- The client-side HP EFS WAN Accelerator is configured as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

### Basic Steps (Server-Side)

Perform the following steps on each of the server-side HP EFS WAN Accelerators.

1. Configure the server-side HP EFS WAN Accelerator as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
3. Navigate to the Setup: Advanced Networking - Connection Forwarding page in the Management Console.
4. Configure each of the neighbors by specifying the in-path IP address for the neighbor HP EFS WAN Accelerator.

**Figure 5-4.** Setup: Advanced Networking - Connection Forwarding Page

◆ Under Add New Entry, type the in-path IP address for the neighbor HP EFS WAN Accelerator in the **Neighbor IP** text box.

◆ Type the neighbor port in the **Neighbor port** text box. The default port is **7850**.

◆ Click **Add Peer** to add the neighbor appliance to your running configuration.

◆ Under Global Settings, click **Enable Connection Forwarding**.

◆ Optionally, you can configure global keep-alive intervals and count for the neighbor HP EFS WAN Accelerators.

◆ Click **Update Settings**.

5. Save the new configuration in the Setup: Configuration Manager page.
6. Restart the HP EFS WAN Accelerator service in the Setup: Start/Stop Services page.
7. Begin optimization. View performance reports and system logs in the Management Console.

# Configuring Connection Forwarding Using the CLI

The following section describes how to enable and configure connection forwarding using the CLI.

To configure connection forwarding you enable the feature and define the HP EFS WAN Accelerator neighbors on each of the server-side HP EFS WAN Accelerators in the network.

## To enable connection forwarding

1. Connect to the CLI. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual*.

2. At the system prompt, enter the following set of commands:

```
HP EFS WAN Accelerator-2> enable
HP EFS WAN Accelerator-2 # configure terminal
HP EFS WAN Accelerator-2 (config) #
HP EFS WAN Accelerator-2 (config) # in-path neighbor enable
HP EFS WAN Accelerator-2 (config) # in-path neighbor ip address 10.0.0.6
    ;;the in-path ip address of HP EFS WAN Accelerator-3
HP EFS WAN Accelerator-2 (config) # write memory
HP EFS WAN Accelerator-2 (config) # restart

HP EFS WAN Accelerator-3> enable
HP EFS WAN Accelerator-3 # configure terminal
HP EFS WAN Accelerator-3 (config) # in-path neighbor enable
HP EFS WAN Accelerator-3 (config) # in-path neighbor ip address 10.0.0.5
    ;;the in-path ip address of HP EFS WAN Accelerator-2
```

## CHAPTER 6

# Policy-Based Routing Deployments

## In This Chapter

This chapter describes how to configure the Policy-Based Routing (PBR) to redirect traffic to an HP EFS WAN Accelerator or group of HP EFS WAN Accelerators. It contains the following sections:

- ◆ “Introduction to PBR,” next
- ◆ “Overview of CDP” on page 46
- ◆ “How PBR works on a Cisco 6500 Platform, Version 12.2(17d) SXB1” on page 47
- ◆ “Connecting the HP EFS WAN Accelerator to Your Network in PBR Deployments” on page 48
- ◆ “Asymmetric HP EFS WAN Accelerator Deployments With PBR” on page 49
- ◆ “Client-Side HP EFS WAN Accelerator Attached to a Router through a Switch” on page 54
- ◆ “Client-Side HP EFS WAN Accelerator Attached to an Inside Router” on page 55
- ◆ “PBR Between VLANs” on page 55
- ◆ “Symmetric HP EFS WAN Accelerator Deployments With PBR and Autodiscovery” on page 57
- ◆ “Symmetric Deployments with PBR, Autodiscovery, and CDP” on page 60

This chapter assumes you are familiar with the HP EFS WAN Accelerator Management Console (Management Console). For detailed information about the Management Console and how to use it, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

This chapter also assumes that you are familiar with the installation and configuration process for the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

This chapter provides the basic steps for PBR network deployments. It does not provide detailed procedures. Use this chapter as a general guide to these deployments. If you need additional assistance, contact HP technical support located at <http://www.hp.com>.

For detailed information about the factors you must consider before you design and deploy the HP EFS WAN Accelerator in a network environment, see “[Design and Deployment Overview](#)” on page 11.

---

## Introduction to PBR

PBR is a router configuration that allows you to define policies to route packets instead of relying on routing protocols. It is enabled on an interface basis and packets coming into a PBR-enabled interface are checked to see if they match the defined policies. If they do match, the packets are applied as the rule defined for the policy. If they do not match, packets are routed based on the usual routing table. The rules redirect the packets to a specific IP address.

Typically, you configure PBR on the client-side of the network to redirect traffic to an HP EFS WAN Accelerator.

---

**IMPORTANT:** PBR must be enabled on the interfaces where the client traffic is arriving and disabled on the interfaces corresponding to the HP EFS WAN Accelerator, to avoid an infinite loop. (The HP EFS WAN Accelerator can bounce back the packets it receives either because it is not configured to optimize that traffic or its admission control is refusing new connections.)

---

On the server-side, the HP EFS WAN Accelerator is configured as, an out-of-path device, although it can also be configured with a PBR router with a specific PBR rule or as an in-path device.

In all cases, the HP EFS WAN Accelerator that intercepts traffic redirected with PBR is configured with in-path support and PBR support enabled. PBR policies can be based on the source IP address, destination IP address, protocol (TCP only), source port, or destination port.

---

## Overview of CDP

CDP is a protocol used by Cisco routers and switches to obtain neighbor IP addresses, model, IOS version, and so forth. The protocol runs at the Open System Interconnection (OSI) layer 2 using the 802.3 Ethernet frame.

HP EFS WAN Accelerators can be deployed in several ways: physically in path, virtually in path, or out of path. Virtual in-path deployments require that a network device redirect packets to the HP EFS WAN Accelerators. Network devices that are capable of redirection are layer-4 switches, WCCP enabled routers and switches, and PBR enabled routers.

Either PBR or WCCP can be used to redirect traffic from a router to an HP EFS WAN Accelerator. On some platforms, such as the Cisco 6509 platform on which WCCP runs, WCCP can only redirect a limited number of TCP ports to the HP EFS WAN Accelerator without reverting to software forwarding. This characteristic has a tendency to spike the Central Processing Unit (CPU) of the router. On Cisco 6500s running IOS 12.x can redirect all TCP ports and do the PBR forwarding in the hardware.

WCCP is designed to redirect traffic to a group of HP EFS WAN Accelerators so it is often better in clustering solutions. With PBR, any clustering must be done by manually by configuring a set of redirect rules. The following table summarizes the advantages and disadvantages of PBR and WCCP.

Capability	Platform	WCCP	PBR
Hardware Redirection of All TCP Connections	Cisco 6500	Limited numbers of TCP ports	All TCP traffic.
Clustering	All	Redirect to a group of HP EFS WAN Accelerators	No groups for redirection. Can be a manual setup.
Failover	All	Will only redirect to active HP EFS WAN Accelerators in a group	Requires CDP on the HP EFS WAN Accelerator to bypass an HP EFS WAN Accelerator that is down.

For an example configuration, see “[Symmetric Deployments with PBR, Autodiscovery, and CDP](#)” on page 60.

---

## How PBR works on a Cisco 6500 Platform, Version 12.2(17d) SXB1

One of the major issues with PBR is that it can *blackhole* traffic (that is, drop all TCP connections to a destination) if the device it is redirecting to fails. To avoid blackholing traffic, PBR must have a way of tracking whether the PBR next hop is available. You can enable this tracking feature in a route map with the following Cisco router command:

```
set ip next-hop verify-availability
```

With this command, PBR attempts to verify the availability of the next hop using information from CDP. If that next hop is unavailable, it skip the actions specified in the route map.

PBR checks availability in the following manner:

1. When PBR first attempts to send to a PBR next hop, it checks the CDP neighbor table to see if the IP address of the next hop appears to be available. If so, it sends

an Address Resolution Protocol (ARP) request for the address, resolves it, and begins redirecting traffic to the next hop (that is, the HP EFS WAN Accelerator).

2. After PBR has verified the next hop, it continues to send to the next hop as long as it obtains answers from the ARP request for the next hop IP address. If the ARP request fails to obtain an answer, it then rechecks the CDP table. If there is no entry in the CDP table, it no longer uses the route map to send traffic. This verification provides a failover mechanism.

---

**NOTE:** Using PBR with CDP will not work on a Cisco 6500 router and switch combination that is setup in hybrid mode. You must use a native setup for this to work. A hybrid setup fails because all the routing is done on the Multilayer Switch Feature Card (MSFC). This card is treated as an independent system in a hybrid setup. Therefore, when you run the **show cdp neighbors** command on the MSFC, it displays the Supervisor card as its only neighbor. It does not see any of the devices that are connected to the switch ports. Therefore, it assumes none of those devices are reachable, and it does not redirect any traffic for route maps that use **set ip next-hop verify-availability**.

---

In more recent versions of the Cisco IOS software, there is a feature called PBR with Multiple Tracking Options. In addition to the old method of using CDP information, it allows methods such as HTTP and **ping** to be used to determine whether the PBR next hop is available. Using CDP allows you to run with older IOS 12.x versions.

---

**NOTE:** CDP is required for failover deployments on Cisco 6000, 6500, and 7600 platforms because Multiple Tracking Options is not available on these platforms.

---

For an example configuration, see “[Symmetric Deployments with PBR, Autodiscovery, and CDP](#)” on page 60.

---

## Connecting the HP EFS WAN Accelerator to Your Network in PBR Deployments

There are two Ethernet cables attached to the HP EFS WAN Accelerator in PBR deployments:

- ◆ A Straight through cable to the **Primary** interface. You use this connection to manage the HP EFS WAN Accelerator, reaching it through HTTPS or SSH.
- ◆ A Straight through cable to the **WAN** interface. You assign an IP address to the In-Path interface; this is the IP address that you redirect traffic to (that is, the target of the router PBR rule).

## Asymmetric HP EFS WAN Accelerator Deployments With PBR

The following section describes asymmetric HP EFS WAN Accelerator deployments with PBR. The examples in this section apply only if the clients are on one side of the WAN and are connecting to servers on the other side of the WAN.

If the client-side HP EFS WAN Accelerator is on a different Layer-2 interface than the clients on the router where PBR is configured, PBR can be enabled on a Layer-2 interface basis, and redirects TCP traffic going to the server.

---

**IMPORTANT:** HP recommends you define a policy based on the source or destination IP and not on the TCP source or destination ports because certain protocols use dynamic ports instead of fixed ones such as Exchange and File Transfer Protocol (FTP).

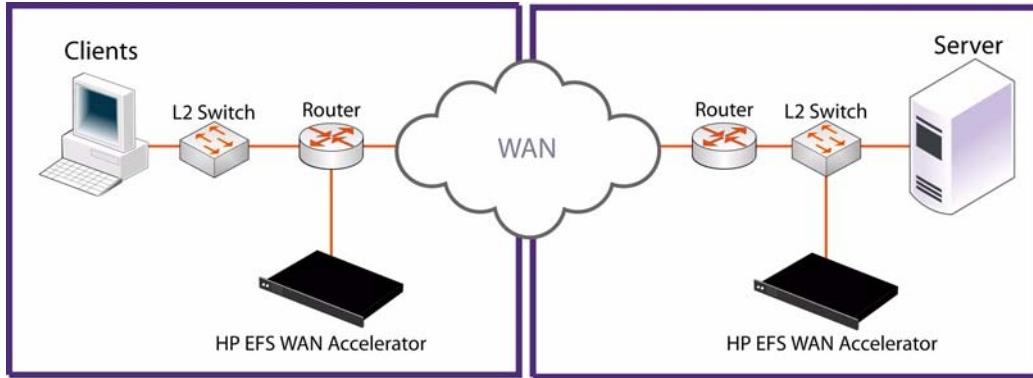
---

### Configuring PBR Using the CLI

The following section describes how to configure PBR using the HP EFS WAN Accelerator command-line interface (CLI).

The following figure illustrates a network where PBR is enabled on the interface of the client-side router connected to the Layer-2 switch that redirects traffic to the HP EFS WAN Accelerator.

**Figure 6-1.** Client-Side, HP EFS WAN Accelerator Attached to a Router



The client-side router has a **fastEthernet 0/0** interface attached to the Layer-2 switch and **fastEthernet0/1** attached to the HP EFS WAN Accelerator.

The server-side router has a **fastEthernet0/0** interface attached to the Layer-2 switch.

This example uses the following IP addresses:

- ◆ **Client-side.** Clients=**10.0.0.0/16**, HP EFS WAN Accelerator=**10.2.0.2/16**, Router(**fastEthernet0/0**)=**10.0.0.1/16**, Router(**fastEthernet0/1**)=**10.2.0.1/16**
- ◆ **Server-side.** Servers=**10.1.0.0/16**, HP EFS WAN Accelerator=**10.1.0.3/16**, Router(**fastEthernet0/0**)=**10.1.0.1/16**

In this example, the HP EFS WAN Accelerator is configured as a client-side, HP EFS WAN Accelerator in an in-path configuration with PBR support. It must reach the remote network through the router from the in-path interface and a fixed-target in-path rule is defined for the remote out-of-path HP EFS WAN Accelerator.

## Basic Steps (Client-Side)

### To configure the client-side HP EFS WAN Accelerator

Perform the following basic steps for the client-side HP EFS WAN Accelerator.

1. Connect to the client-side CLI. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual*.
2. On the client-side HP EFS WAN Accelerator, at the system prompt, enter the following set of commands:

```
client-SH > enable
client-SH # configure terminal
client-SH (config) # in-path enable
client-SH (config) # in-path oop enable
client-SH (config) # interface in-path ip address 10.2.0.2 /16
client-SH (config) # ip in-path-gateway inpath0_0 10.2.0.1
client-SH (config) # in-path rule fixed-target dstaddr 10.1.0.0/16
dstport 135 target-addr 10.1.0.3
client-SH (config) # in-path rule fixed-target dstaddr 10.1.0.0/16
dstport 139 target-addr 10.1.0.3
client-SH (config) # in-path rule fixed-target dstaddr 10.1.0.0/16
dstport 445 target-addr 10.1.0.3
client-SH (config) # in-path rule fixed-target dstaddr 10.1.0.0/16
dstport 21 target-addr 10.1.0.3
client-SH (config) # in-path rule fixed-target dstaddr 10.1.0.0/16
dstport 80 target-addr 10.1.0.3
client-SH (config) # write memory
client-SH (config) # restart
```

---

**NOTE:** You must save your changes to memory and restart the HP EFS WAN Accelerator for your changes to take effect.

---

This configuration optimizes Common Internet File System (CIFS), Exchange, FTP, and Hypertext Transfer Protocol (HTTP) traffic.

### To configure the client-side router

- On the client-side router, at the system prompt, enter the following set of commands:

```
Router#configure terminal
Router(config)#access-list 101 permit tcp any 10.1.0.0 0.0.255.255
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.0.0.1 255.255.0.0
Router(config-if)#ip policy route-map TrafficToS
Router(config-if)#exit
Router(config)#route-map TrafficToS permit 10
Router(config-route-map)#match ip address 101
Router(config-route-map)#set ip next-hop 10.2.0.2
Router(config-route-map)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 10.2.0.1 255.255.0.0
Router(config-if)#end
```

Router#

---

**TIP:** Enter configuration commands, one per line. End with CRTL-Z.

---

The Access Control List (ACL) defines the matching criteria. The route-map defines the action corresponding to the matching criteria. The **ip policy route-map** command attaches a route-map to an interface.

For detailed information about configuring Cisco routers for PBR, see [http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_configuration\\_guide\\_chapter09186a00800c60d2.html#23550](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800c60d2.html#23550).

## **Basic Steps (Server-Side)**

In this example, the server-side HP EFS WAN Accelerator is configured as an out-of-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

## **Configuring PBR Using the Management Console**

The following section describes the basic steps for configuring PBR using the Management Console.

## **Basic Steps (Client-Side)**

Perform the following steps for each client-side HP EFS WAN Accelerator.

1. Configure the HP EFS WAN Accelerator as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
3. Navigate to the Setup: Optimization Service - General Settings page in the Management Console.
4. To enable PBR support, click **Enable In-Path Support, Enable L4/PBR/WCCP Support on Interface wan0\_0** and **Enable Optimizations on inpath0\_0, and inpath0\_1**.

**Figure 6-2.** Setup: Optimization Service - General Settings Page

The screenshot shows the 'Optimization Service - General Settings' page. The left sidebar has a dark background with white text, listing various service and management options. The main content area has a light gray background with sections for 'In-Path' and 'Out-of-Path'. The 'In-Path' section contains several checkboxes, some of which are checked. The 'Out-of-Path' section contains one checkbox. At the bottom right of the main content area are three buttons: 'Apply', 'Save', and 'Reset'. The status bar at the top center says 'Status: Healthy'.

5. Navigate to the Setup: Optimization Service - In-Path Rules page.
6. Define fixed-target, in-path rules to reach the remote network through the remote out-of-path HP EFS WAN Accelerator.

**Figure 6-3.** Setup: Optimization Service - In-Path Rules Page

#	Type	Source	Destination	Port	Target	Port	Opt Policy	Neural	VLAN
1	Pass	All	All	Secure	--	--	--	--	All
2	Pass	All	All	Interactive	--	--	--	--	All
def	Auto	All	All	All	--	--	Normal	Always	All

Add New Rule:

Type: Fixed-Target Insert Rule At: end

Source Subnet: 0.0.0.0/0 Destination Subnet: 0.0.0.0/0 Port: all

Targets:

Target Appliance IP: 10.0.0.4 Port: 7810

Backup Appliance IP: 10.0.0.3 Port: 7810

Advanced Options (click to open):

VLAN Tag ID: All Optimization Policy: Normal Neural Framing Mode: Always

Add Rule

Additional Options:

Enable Computation of Neural Heuristics

Update Settings

Save Reset

7. Apply and save the new configuration in the Setup: Configuration Manager page.
8. Restart the HP EFS WAN Accelerator service in the Setup: Start/Stop Services page.
9. Begin optimization. View performance reports and system logs in the Management Console.

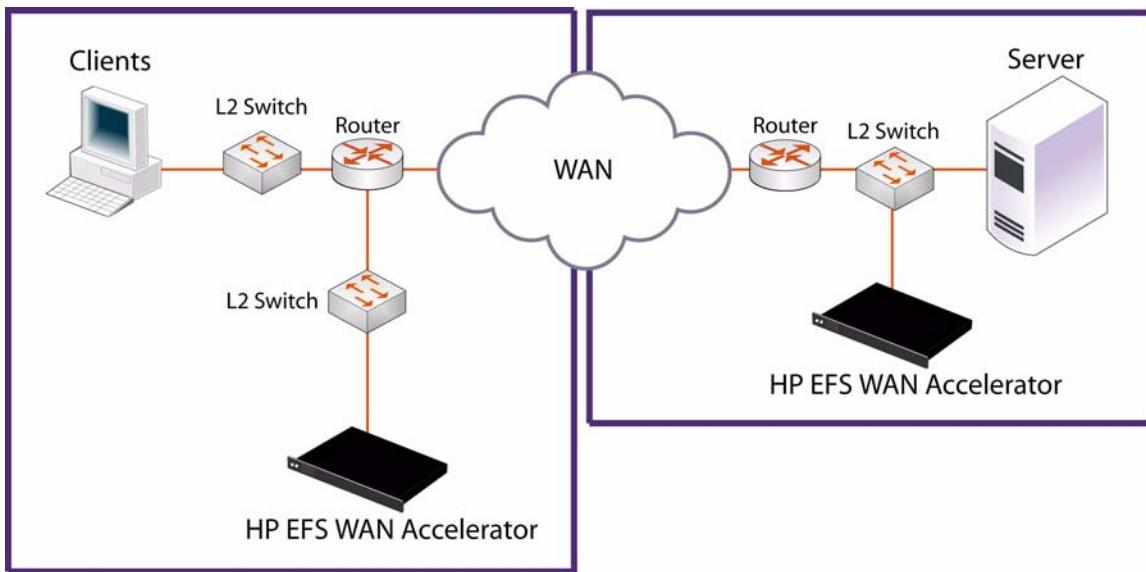
## Basic Steps (Server-Side)

The server-side HP EFS WAN Accelerator is configured as an out-of-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

## Client-Side HP EFS WAN Accelerator Attached to a Router through a Switch

In this deployment, PBR is enabled on the interface of the client-side router connected to the Layer-2 switch that redirects traffic to the HP EFS WAN Accelerator. Communication between the client-side HP EFS WAN Accelerator and the clients must be through the client-side router.

**Figure 6-4.** Client-Side HP EFS WAN Accelerator Attached to a Router through a Switch



### Basic Steps (Client-Side)

Perform the steps for “[Basic Steps \(Client-Side\)](#)” on page 50.

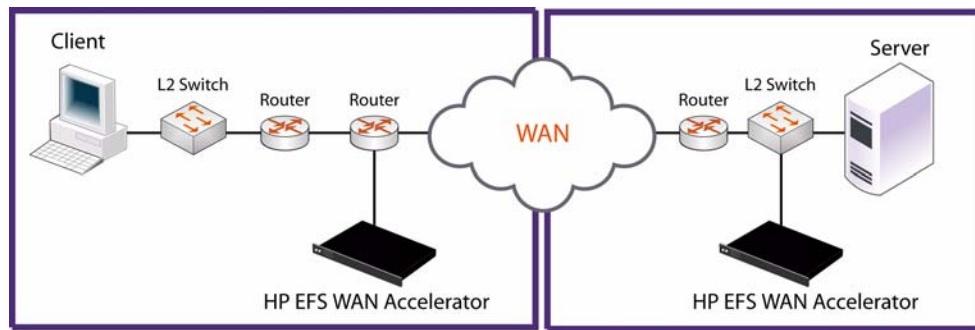
### Basic Steps (Server-Side)

Perform the steps for “[Basic Steps \(Server-Side\)](#)” on page 51.

## Client-Side HP EFS WAN Accelerator Attached to an Inside Router

In this deployment, PBR is enabled on the router interface connected to the Layer-2 switch that redirects traffic to the HP EFS WAN Accelerator. The same PBR rules should not be enabled on the WAN router (or any other router on the way to the WAN).

**Figure 6-5.** Client-Side HP EFS WAN Accelerator Attached to an Inside Router



### Basic Steps (Client-Side)

Perform the steps for “[Basic Steps \(Client-Side\)](#)” on page 50. Make sure that you configure different PBR rules for the second router.

### Basic Steps (Server-Side)

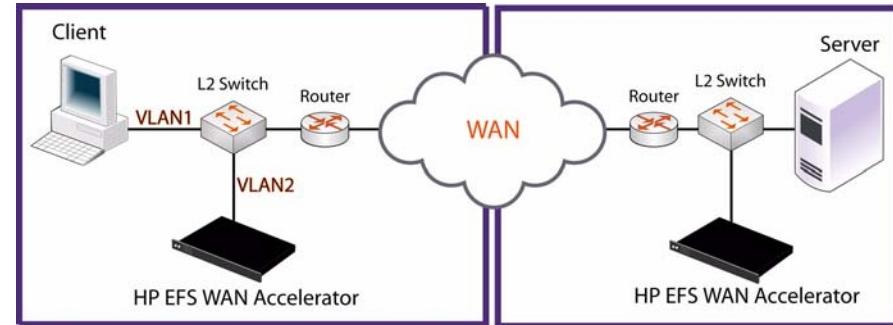
Perform the steps for “[Basic Steps \(Server-Side\)](#)” on page 51.

## PBR Between VLANs

If there is not a clear physical separation between the client and the HP EFS WAN Accelerator on the router where PBR is defined, you can use Virtual Local Area Networks (VLANs) to create a virtual separation.

In the following figure, the HP EFS WAN Accelerator is configured in a different VLAN than the client VLAN, and PBR is enabled on the client VLAN interface and disabled on the HP EFS WAN Accelerator VLAN interface.

**Figure 6-6.** PBR Between VLANs



In this configuration, the HP EFS WAN Accelerator is attached to any Layer-2 switch that the router can reach (even the same switch as the clients). VLAN trunking is enabled between the Layer-2 switch and the PBR router (not on the link between the HP EFS WAN Accelerator and the switch).

In this configuration you use the IP addresses in a single subnet and the router has 2 VLAN interfaces on **fastEthernet0/0**.

### To configure the HP EFS WAN Accelerator

Use the procedures in “[Basic Steps \(Client-Side\)](#)” on page 50. With a single subnet configuration, the route-map is attached to a VLAN interface instead of an ethernet interface.

This example assumes that VLAN trunking is already configured on the Layer-2 switch and the router for the clients VLAN (**VLAN1**) and that the Layer-2 switch configuration for **VLAN2** is already completed.

### To configure the Cisco router

- On the client-side router, at the system prompt, enter the following set of commands:

```
Router#configure terminal
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 10.2.0.1 255.255.0.0
Router(config-subif)#exit
Router(config)#access-list 101 permit tcp any 10.1.0.0 0.0.255.255
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q 1
Router(config-subif)#ip address 10.0.0.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToS
Router(config-subif)#exit
Router(config)#route-map TrafficToS permit 10
Router(config-route-map)#match ip address 101
Router(config-route-map)#set ip next-hop 10.2.0.2
Router(config-route-map)#end
Router#
```

---

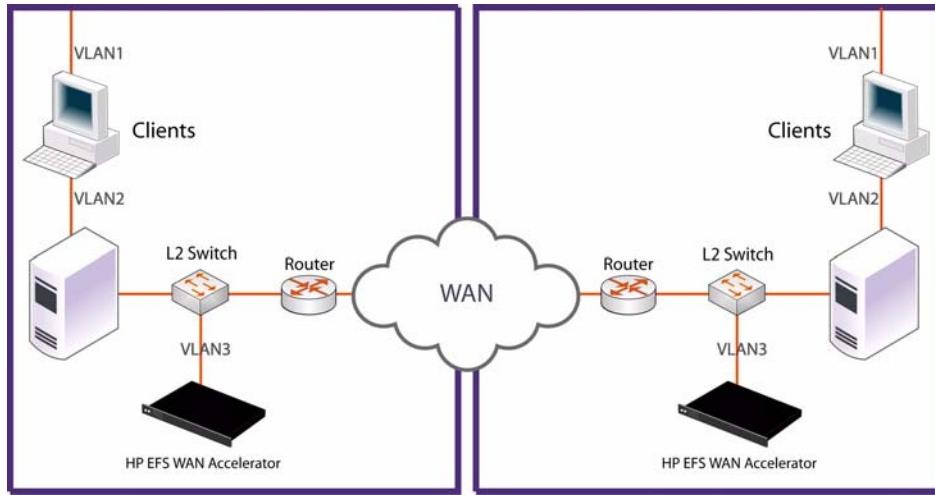
**TIP:** Enter configuration commands, one per line. End with CTRL-Z.

---

## Symmetric HP EFS WAN Accelerator Deployments With PBR and Autodiscovery

In the case where clients and servers are on both sides of the WAN, PBR can be configured on both sides of the network where each router has the reversed rules of the other router.

**Figure 6-7.** Symmetric HP EFS WAN Accelerator Deployments with PBR



For this example, assume that clients, servers, and HP EFS WAN Accelerators are all on a separate VLANs and the Layer-2 switch is attached to the router **fastEthernet0/0** interface. This example uses the following IP addresses:

- ◆ **Left-side.** Clients=10.0.1.0/24, Servers=10.0.2.0/24, HP EFS WAN Accelerator=10.0.3.0/24
- ◆ **Right-side.** Clients=10.1.1.0/24, Servers=10.1.2.0/24, HP EFS WAN Accelerator=10.1.3.0/24

Each router is connected to the WAN through their Fast Ethernet 0/1 interfaces. They use the following IP addresses:

- ◆ Left WAN = 10.0.4.0/24
- ◆ Right WAN = 10.1.4.0/24

### To configure the HP EFS WAN Accelerators

1. On the left HP EFS WAN Accelerator, at the system prompt, enter the following set of commands:

```
Left-SH > enable
Left-SH # configure terminal
Left-SH (config) # in-path enable
Left-SH (config) # in-path oop enable
Left-SH (config) # interface in-path ip address 10.0.3.2 /24
Left-SH (config) # ip in-path-gateway inpath0_0 10.0.3.1
Left-SH (config) # write memory
Left-SH (config) # restart
```

2. On the right HP EFS WAN Accelerator, at the system prompt, enter the following set of commands:

```

Right-SH > enable
Right-SH # configure terminal
Right-SH (config) # in-path enable
Right-SH (config) # in-path oop enable
Right-SH (config) # interface in-path ip address 10.1.3.2 /24
Right-SH (config) # ip in-path-gateway inpath0_0 10.1.3.1
Right-SH (config) # write memory
Right-SH (config) # restart

```

---

**IMPORTANT:** You must save your changes to memory and restart the HP EFS WAN Accelerator service for your changes to take effect.

---

## To configure the Cisco router

1. On the left router, at the system prompt, enter the following commands:

---

**TIP:** Enter configuration commands, one per line; end with CTRL-Z.

---

```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q 1
Router(config-subif)#ip address 10.0.1.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToRights
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 10.0.2.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficFromLefts
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 10.0.3.1 255.255.0.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/1
Router(config-subif)#ip address 10.0.4.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToLeftSAndFromRights
Router(config-subif)#exit
Router(config)#access-list 101 permit tcp any 10.1.2.0 0.0.0.255
Router(config)#access-list 102 permit tcp 10.0.2.0 0.0.0.255 any
Router(config)#access-list 103 permit tcp any 10.0.2.0 0.0.0.255
Router(config)#access-list 104 permit tcp 10.1.2.0 0.0.0.255 any
Router(config)#route-map TrafficToRights permit 10
Router(config-route-map)#match ip address 101
Router(config-route-map)#set ip next-hop 10.0.3.2
Router(config-route-map)#exit
Router(config)#route-map TrafficFromLefts permit 10
Router(config-route-map)#match ip address 102
Router(config-route-map)#set ip next-hop 10.0.3.2
Router(config-route-map)#exit
Router(config)#route-map TrafficToLeftSAndFromRights permit 10
Router(config-route-map)#match ip address 103 104
Router(config-route-map)#set ip next-hop 10.0.3.2
Router(config-route-map)#end
Router#

```

2. On the right router, at the system prompt, enter the following set of commands:

```

Router#configure terminal
Router(config)#interface fastEthernet 0/0.1

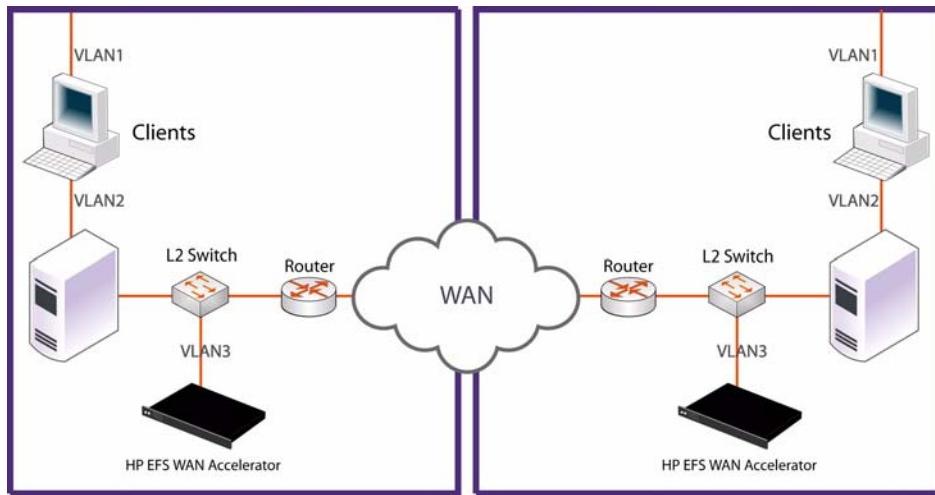
```

```
Router(config-subif)#encapsulation dot1Q 1
Router(config-subif)#ip address 10.1.1.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToLeftS
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 10.1.2.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficFromRights
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 10.1.3.1 255.255.0.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/1
Router(config-subif)#ip address 10.1.4.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToRightSAndFromLeftS
Router(config-subif)#exit
Router(config)#access-list 101 permit tcp any 10.0.2.0 0.0.0.255
Router(config)#access-list 102 permit tcp 10.1.2.0 0.0.0.255 any
Router(config)#access-list 103 permit tcp any 10.1.2.0 0.0.0.255
Router(config)#access-list 104 permit tcp 10.0.2.0 0.0.0.255 any
Router(config)#route-map TrafficToLeftS permit 10
Router(config-route-map)#match ip address 101
Router(config-route-map)#set ip next-hop 10.1.3.2
Router(config-route-map)#exit
Router(config)#route-map TrafficFromRights permit 10
Router(config-route-map)#match ip address 102
Router(config-route-map)#set ip next-hop 10.1.3.2
Router(config-route-map)#exit
Router(config)#route-map TrafficToRightSAndFromLeftS permit 10
Router(config-route-map)#match ip address 103 104
Router(config-route-map)#set ip next-hop 10.1.3.2
Router(config-route-map)#end
Router#
```

## Symmetric Deployments with PBR, Autodiscovery, and CDP

In the case where clients and servers are on both sides of the WAN, PBR can be configured on both sides of the network where each router has the reversed rules of the other router.

**Figure 6-8.** Symmetric HP EFS WAN Accelerator Deployments with PBR



For this example, assume that clients, servers, and HP EFS WAN Accelerators are all on a separate VLANs and the Layer-2 switch is attached to the router **fastEthernet0/0** interface. This example uses the following IP addresses:

- ◆ **Left-side.** Clients=10.0.1.0/24, Servers=10.0.2.0/24, HP EFS WAN Accelerator=10.0.3.0/24
- ◆ **Right-side.** Clients=10.1.1.0/24, Servers=10.1.2.0/24, HP EFS WAN Accelerator=10.1.3.0/24

Each router is connected to the WAN through their Fast Ethernet 0/1 interfaces. They use the following IP addresses:

- ◆ Left WAN = 10.0.4.0/24
- ◆ Right WAN = 10.1.4.0/24

### To configure the HP EFS WAN Accelerators

1. On the left HP EFS WAN Accelerator, at the system prompt, enter the following set of commands:

```
Left-SH > enable
Left-SH # configure terminal
Left-SH (config) # in-path enable
Left-SH (config) # in-path oop enable
Left-SH (config) # in-path cdp enable
Left-SH (config) # interface in-path ip address 10.0.3.2 /24
Left-SH (config) # ip in-path-gateway inpath0_0 10.0.3.1
Left-SH (config) # write memory
Left-SH (config) # restart
```

2. On the right HP EFS WAN Accelerator, at the system prompt, enter the following set of commands:

```

Right-SH > enable
Right-SH # configure terminal
Right-SH (config) # in-path enable
Right-SH (config) # in-path oop enable
Right-SH (config) # in-path cdp enable
Right-SH (config) # interface in-path ip address 10.1.3.2 /24
Right-SH (config) # ip in-path-gateway inpath0_0 10.1.3.1
Right-SH (config) # write memory
Right-SH (config) # restart

```

**IMPORTANT:** You must save your changes to memory and restart the HP EFS WAN Accelerator service for your changes to take effect.

## To configure the Cisco router

- On the left router, at the system prompt, enter the following commands:

**TIP:** Enter configuration commands, one per line; end with CTRL-Z.

```

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q 1
Router(config-subif)#ip address 10.0.1.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToRights
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 10.0.2.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficFromLefts
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 10.0.3.1 255.255.0.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/1
Router(config-subif)#ip address 10.0.4.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToLeftSAndFromRights
Router(config-subif)#exit
Router(config)#access-list 101 permit tcp any 10.1.2.0 0.0.0.255
Router(config)#access-list 102 permit tcp 10.0.2.0 0.0.0.255 any
Router(config)#access-list 103 permit tcp any 10.0.2.0 0.0.0.255
Router(config)#access-list 104 permit tcp 10.1.2.0 0.0.0.255 any
Router(config)#route-map TrafficToRights permit 10
Router(config-route-map)#match ip address 101
Router(config-route-map)#set ip next-hop 10.0.3.2
Router(config-route-map)#set ip next-hop verify-availability
Router(config-route-map)#exit
Router(config)#route-map TrafficFromLefts permit 10
Router(config-route-map)#match ip address 102
Router(config-route-map)#set ip next-hop 10.0.3.2
Router(config-route-map)#set ip next-hop verify-availability
Router(config-route-map)#exit
Router(config)#route-map TrafficToLeftS permit 10
Router(config-route-map)#match ip address 103 104
Router(config-route-map)#set ip next-hop 10.0.3.2
Router(config-route-map)#set ip next-hop verify-availability
Router(config-route-map)#end
Router#

```

- On the right router, at the system prompt, enter the following set of commands:

```

Router#configure terminal
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q 1
Router(config-subif)#ip address 10.1.1.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToLeftS
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 10.1.2.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficFromRights
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 10.1.3.1 255.255.0.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/1
Router(config-subif)#ip address 10.1.4.1 255.255.0.0
Router(config-subif)#ip policy route-map TrafficToRightSAndFromLeftS
Router(config-subif)#exit
Router(config)#access-list 101 permit tcp any 10.0.2.0 0.0.0.255
Router(config)#access-list 102 permit tcp 10.1.2.0 0.0.0.255 any
Router(config)#access-list 103 permit tcp any 10.1.2.0 0.0.0.255
Router(config)#access-list 104 permit tcp 10.0.2.0 0.0.0.255 any
Router(config)#route-map TrafficToLeftS permit 10
Router(config-route-map)#match ip address 101
Router(config-route-map)#set ip next-hop 10.1.3.2
Router(config-route-map)#set ip next-hop verify-availability
Router(config-route-map)#exit
Router(config)#route-map TrafficFromRights permit 10
Router(config-route-map)#match ip address 102
Router(config-route-map)#set ip next-hop 10.1.3.2
Router(config-route-map)#set ip next-hop verify-availability
Router(config-route-map)#exit
Router(config)#route-map TrafficToRights permit 10
Router(config-route-map)#match ip address 103 104
Router(config-route-map)#set ip next-hop 10.1.3.2
Router(config-route-map)#set ip next-hop verify-availability
Router(config-route-map)#end
Router#

```

---

## Troubleshooting

On Cisco routers with Internet Operating System (IOS) version 12.3T, the PBR support for Multiple Tracking Options feature allows the router to check if a machine is still functioning. This feature can detect if the HP EFS WAN Accelerator is up and, if not, to stop redirecting the traffic to it.

You can use the following methods to check an HP EFS WAN Accelerator:

- ◆ Internet Control Message Protocol (ICMP) **ping** reachability to a remote device.
- ◆ Application running on a remote device (for example, the device responds to an **HTTP GET** request).
- ◆ A route exists in the Routing Information Base (RIB) (for example, policy route only if **10.2.2.0/24** is in the RIB).
- ◆ Interface state (for example, packets received on **E0** should be the policy routed out of **E1** only if **E2** is down).

## CHAPTER 7

# WCCP Deployments

## In This Chapter

This chapter describes how to configure the Web Cache Communication Protocol (WCCP) to redirect traffic to an HP EFS WAN Accelerator or group of HP EFS WAN Accelerators. It contains the following sections:

- ◆ “Introduction to WCCP,” next
- ◆ “Connecting the HP EFS WAN Accelerator to Your Network in WCCP Deployments” on page 67
- ◆ “A Basic WCCP Configuration” on page 68
- ◆ “Configuring WCCP Using the Management Console” on page 70
- ◆ “Dual WCCP Deployment” on page 76
- ◆ “Additional WCCP Features” on page 79
- ◆ “Troubleshooting” on page 82

This chapter assumes you are familiar with the HP EFS WAN Accelerator Management Console (Management Console). For detailed information about the Management Console and how to use it, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

This chapter also assumes that you are familiar with the installation and configuration process for the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

This chapter provides the basic steps for WCCP network deployments. It does not provide detailed procedures. Use this chapter as a general guide to these deployments. If you need additional assistance, contact HP technical support located at <http://www.hp.com>.

For detailed information about the factors you must consider before you design and deploy the HP EFS WAN Accelerator in a network environment, see “[Design and Deployment Overview](#)” on page 11.

## Introduction to WCCP

WCCP was originally implemented on Cisco routers, multi-layer switches, and Web caches to redirect HTTP requests to local Web caches (Version 1). Version 2, which is implemented on HP EFS WAN Accelerators, can redirect any type of connection from multiple routers to multiple Web caches.

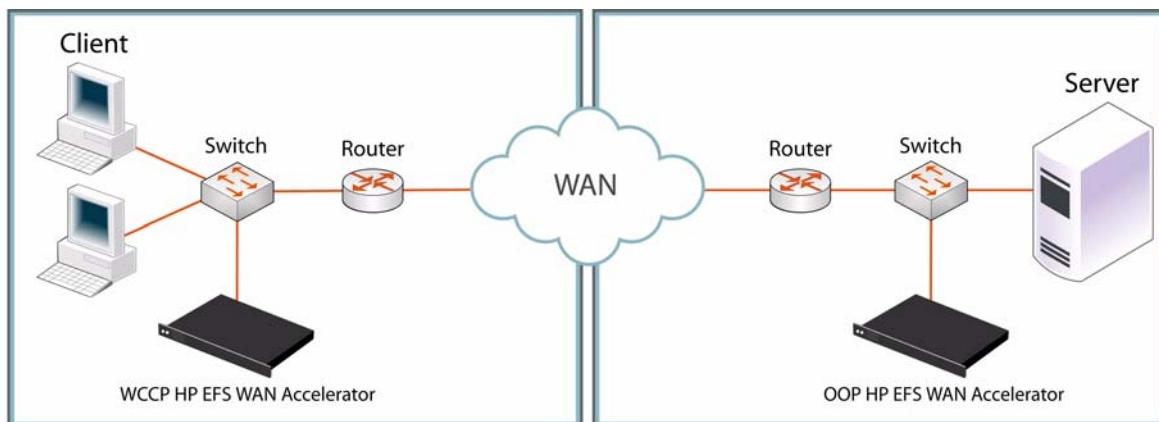
You configure WCCP to redirect traffic to an HP EFS WAN Accelerator or group of HP EFS WAN Accelerators:

- ◆ so that the HP EFS WAN Accelerators do not have to be *physically in-path* but can be *virtually in-path*. That is, the HP EFS WAN Accelerators are configured to be physically out-of-path devices while optimizing traffic as if they were in-path devices.
- ◆ to redirect traffic to an HP EFS WAN Accelerator or group of HP EFS WAN Accelerators to provide load balancing and failover support.

You can configure WCCP on the client-side HP EFS WAN Accelerator or the server-side HP EFS WAN Accelerator. They can be in-path devices or out-of-path devices, depending on your network environment.

The following figure illustrates WCCP configured on the client-side and an out-of-path HP EFS WAN Accelerator on the server-side. This is an example of one type of WCCP deployment. Contact HP technical support for further information at <http://www.hp.com>.

**Figure 7-1. Basic WCCP Configuration**



The following steps describe how WCCP works with the HP EFS WAN Accelerator:

1. Routers and HP EFS WAN Accelerators are added to the same service group.
2. HP EFS WAN Accelerators announce themselves to the routers.
3. Routers send back the state of the service group.
4. One HP EFS WAN Accelerator takes a leadership role and tells the routers how to redirect traffic among the HP EFS WAN Accelerators in the service group.

The HP EFS WAN Accelerators use the following methods to communicate with routers:

- ◆ **Unicast (User Datagram Protocol Packets).** The HP EFS WAN Accelerator is configured with the IP address of each router. If additional routers are added to the service group, they must be added on each HP EFS WAN Accelerator.
- ◆ **Multicast.** The HP EFS WAN Accelerator is configured with a multicast group. If additional routers are added, you do not need to add or change configuration settings on the HP EFS WAN Accelerators.

All Transmission Control Traffic (TCP) traffic is redirected by default. You can configure specific source or destination ports to be redirected. For detailed information, see “[TCP Port Redirection](#)” on page 80.

For other types of redirection filtering such as the Internet Protocol (IP) address, you configure Access Control Lists (ACLs) on the routers and add it to the service group. For detailed information, see “[Specific Traffic Redirection](#)” on page 81.

Traffic is redirected using one of the following schemes:

- ◆ **gre (Generic Routing Encapsulation).** Each data packet is encapsulated in a GRE packet with the HP EFS WAN Accelerator IP address configured as the destination. This scheme is applicable to any network.
- ◆ **l2 (Layer-2).** Each packet Media Access Control (MAC) address is rewritten with an HP EFS WAN Accelerator MAC address. This scheme is possible only if the HP EFS WAN Accelerator is connected to a router at Layer-2.
- ◆ **either.** The **either** value uses l2 (Layer-2) first—if Layer-2 is not supported, **gre** is used.

You can load-balance using WCCP. Traffic is redirected based on a hashing scheme and the weight of the HP EFS WAN Accelerators. You can hash on a combination of the source IP address, destination IP address, source port, or destination port. The default weight is based on the HP EFS WAN Accelerator model number. (The weight is heavier for models that support more connections.) You can modify the default weight. For detailed information, see “[Load Balancing](#)” on page 81.

You can also provide failover support using WCCP. In a failover configuration, the HP EFS WAN Accelerators periodically announce themselves to the routers. If an HP EFS WAN Accelerator fails, traffic is redirected to the working HP EFS WAN Accelerators. To configure failover support where the passive HP EFS WAN Accelerator takes over if there is a failure in the active HP EFS WAN Accelerator, you simply configure the weight for the backup HP EFS WAN Accelerator to be **0**. For detailed information, see “[Failover Support](#)” on page 81.

## Basic Steps

The following steps summarize how to configure WCCP on a client-side HP EFS WAN Accelerator with an out-of-path server-side HP EFS WAN Accelerator.

---

**IMPORTANT:** This is an example of one type of WCCP deployment. You can also have deployments with both HP EFS WAN Accelerators configured as in-path devices and WCCP configured on one of them. Contact HP technical support for further information at <http://www.hp.com>.

---

1. Create a service group on the router and set the router to redirect traffic to the HP EFS WAN Accelerator using WCCP on the interfaces where traffic goes.
2. Attach the WAN interface of the HP EFS WAN Accelerator to the network. The WAN interface must be able to communicate with the switch or router where WCCP is configured and where WCCP redirection will take place.
3. Configure the HP EFS WAN Accelerator to be an in-path device with WCCP support on the client-side. For example, **in-path oop enable**.
4. Add fixed-target, in-path rules to reach the server-side HP EFS WAN Accelerator.
5. Add the service group on the HP EFS WAN Accelerator.
6. Enable WCCP on the HP EFS WAN Accelerator.

## **WCCP CLI Commands**

This section summarizes the WCCP commands. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual*.

- ◆ To enable client-side WCCP:

```
SH (config) # wccp enable
```

- ◆ To disable client-side WCCP:

```
SH (config) # no wccp enable
```

- ◆ To specify the multicast Time To Live (ttl) value for WCCP:

```
SH (config) # wccp mcast-ttl 10
```

- ◆ To configure a service group:

```
SH (config) # wccp service-group <service ID> routers <IP address>
[flags] [priority] [ports] [password] [weight] [encap_scheme]
```

<b>service group &lt;service ID&gt;</b>	Specifies the service group identification number (ID) (from <b>0</b> to <b>255</b> ). The service group ID is the number that is set on the router. A value of <b>0</b> specifies the standard http service group which redirects only HTTP traffic.
<b>router &lt;ip_address&gt;</b>	The router IP is a multicast group IP address or a unicast router IP address. A total of 32 routers can be specified.
<b>flags &lt;hash-bit-identifier&gt;</b>	Specifies the combination of <b>src-ip-hash</b> , <b>dst-ip-hash</b> , <b>src-port-hash</b> , <b>dst-port-hash</b> , <b>ports-dest</b> , <b>ports-source</b> that define the fields the router hashes on and if certain ports should be redirected.
<b>ports &lt;portnumber&gt;</b>	Specifies a comma separated list of up to seven ports that the router will redirect. Use only if <b>ports-dest</b> or <b>ports-source</b> service flag is set.
<b>priority &lt;priority-number&gt;</b>	Specifies the WCCP priority for traffic redirection. If a connection matches multiple service groups on a router, the router chooses the service group with the highest priority. The range is <b>0-255</b> . The default value is <b>200</b> .
<b>password &lt;string&gt;</b>	Specifies the WCCP password. This password must be the same as the password on the router. (WCCP requires that all routers in a service group have the same password.) Passwords are limited to 8 characters.
<b>weight &lt;value&gt;</b>	The weight determines how often the traffic is redirected to a particular HP EFS WAN Accelerator. A higher weight redirects more traffic to that HP EFS WAN Accelerator. The ratio of traffic redirected to an HP EFS WAN Accelerator is equal to its weight divided by the sum of the weights of all the HP EFS WAN Accelerators in the same service group. For example, if there are two HP EFS WAN Accelerators in a service group and one has a weight of <b>100</b> and the other has a weight of <b>200</b> , the one with the weight <b>100</b> receives 1/3 of the traffic and the other receives 2/3 of the traffic. The range is <b>0-65535</b> . The default value corresponds to the number of TCP connections your appliance supports.
<b>encap_scheme &lt;string&gt;</b>	Specifies the traffic forwarding and redirection scheme: GRE encapsulation ( <b>gre</b> ) or Layer-2 ( <b>l2</b> ) redirection. The <b>either</b> value uses Layer-2 first—if Layer-2 is not supported, <b>gre</b> is used.

## Connecting the HP EFS WAN Accelerator to Your Network in WCCP Deployments

There are two Ethernet cables attached to the HP EFS WAN Accelerator in WCCP deployments:

- ◆ A Straight through cable to the **Primary** interface. You use this connection to manage the HP EFS WAN Accelerator, reaching it through HTTPS or SSH.
- ◆ A Straight through cable to the **WAN** interface. You assign an IP address to the In-Path interface; this is the IP address that you redirect traffic to.

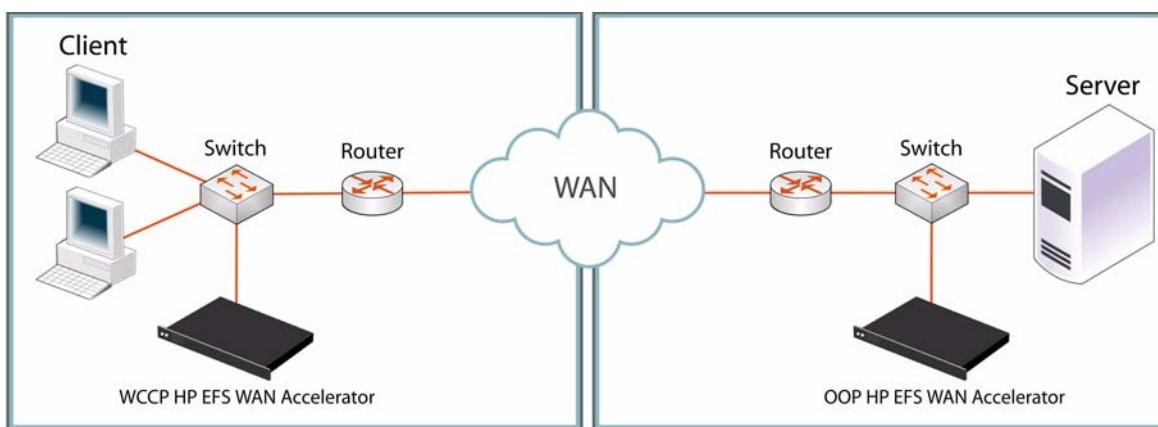
## A Basic WCCP Configuration

This section describes how to configure a router and the HP EFS WAN Accelerator to use WCCP to redirect traffic in a single subnet using the CLI.

You can also use the Management Console to configure the HP EFS WAN Accelerator to use WCCP. In this example the server-side is assumed to be out-of-path.

**IMPORTANT:** This is an example of one type of WCCP deployment. You can also have deployments with both HP EFS WAN Accelerators configured as in-path devices and WCCP configured on one of them.

**Figure 7-2.** Basic WCCP Configuration



### Connecting the HP EFS WAN Accelerator

To set up an HP EFS WAN Accelerator for WCCP, the HP EFS WAN Accelerator WAN interface is connected to a switch or router (not necessarily the one configured for WCCP) that can reach the switch or router where WCCP is configured and where redirection will occur.

**IMPORTANT:** When you connect to the WAN port on the HP EFS WAN Accelerator for WCCP, the LAN port no longer passes traffic. You cannot run the HP EFS WAN Accelerator in both in-path and client, out-of-path mode.

### Configuring the WCCP Router or Multi-Layer Switch

Before you configure the HP EFS WAN Accelerator, you enable your router for WCCP. You create a service group and attach it to the interface where you want packets to be redirected.

In this example, you configure unicast protocol messages between the router and the HP EFS WAN Accelerator and all traffic is redirected to the HP EFS WAN Accelerator. (The HP EFS WAN Accelerator tells the router to redirect TCP traffic and, if configured on it, certain TCP ports.)

The service group ID is **90** and the interface with packets coming from the LAN is **fastEthernet0/0**.

---

**IMPORTANT:** HP recommends that you redirect packets coming into the LAN interface of the router with the **redirect in** feature on the router instead of the **redirect out** feature on the WAN interface of the router so that packets do not go through the routing code twice on the router. Only use the **redirect out** feature if it is impossible to use the **redirect in** feature.

---

### To configure the WCCP router

- At the system prompt, enter the following set of commands:

```
Router> enable
Router# configure terminal
Router(config)# ip wccp version 2
Router(config)# ip wccp 90
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip wccp 90 redirect in
Router(config-if)# end
Router#
```

---

**TIP:** Enter configuration commands, one per line. End with CRTL-Z.

---

The service group **90** must be defined and configured on the HP EFS WAN Accelerator.

## Configuring the Client-Side HP EFS WAN Accelerator

### To configure the HP EFS WAN Accelerator

You configure the client-side HP EFS WAN Accelerator to be an in-path device with WCCP support and you add the service group (that you defined on the router) to it.

In this example, the client-side, in-path HP EFS WAN Accelerator IP address is **10.1.0.2**, its WAN router is **10.1.0.1**, and the server-side HP EFS WAN Accelerator primary IP address is **10.2.0.2**.

- Connect to the HP EFS WAN Accelerator CLI. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual*.
- At the system prompt, enter the following set of commands:

```
client-SH > enable
client-SH # configure terminal
client-SH (config) # in-path enable
client-SH (config) # in-path oop enable
client-SH (config) # interface in-path ip address 10.1.0.2 /16
client-SH (config) # ip in-path-gateway 10.1.0.1
client-SH (config) # write memory
client-SH (config) # restart
```

In this example, you configure the client-side HP EFS WAN Accelerator to optimize ports **135**, **139**, **445**, **21**, and **80** and to pass through all other traffic.

### To add in-path rules to reach the out-of-path, server-side, HP EFS WAN Accelerator

- At the system prompt, enter the following set of commands:

```
client-SH > enable
client-SH # configure terminal
```

```

client-SH (config) # in-path rule fixed-target port 135 target-addr
10.2.0.2
client-SH (config) # in-path rule fixed-target port 139 target-addr
10.2.0.2
client-SH (config) # in-path rule fixed-target port 445 target-addr
10.2.0.2
client-SH (config) # in-path rule fixed-target port 21 target-addr
10.2.0.2
client-SH (config) # in-path rule fixed-target port 80 target-addr
10.2.0.2
client-SH (config) # in-path rule pass-through
client-SH (config) # write memory
client-SH (config) # exit

```

Now add the service group to the HP EFS WAN Accelerator so that the router starts redirecting packets.

#### To add the WCCP service group to the HP EFS WAN Accelerator

- At the system prompt, enter the following set of commands:

```

client-SH > enable
client-SH # configure terminal
client-SH (config) # wccp enable
client-SH (config) # wccp service-group 90 routers 10.1.0.1
client-SH (config) # write memory
client-SH (config) # restart

```

This set of commands instructs the router to redirect all TCP traffic to the HP EFS WAN Accelerator.

## Configuring WCCP Using the Management Console

The following section describes the basic steps for configuring the HP EFS WAN Accelerator using the Management Console.

This section does not describe how you enable your router for WCCP and create a service group for the HP EFS WAN Accelerator. For detailed information about configuring your router, see “[Configuring the WCCP Router or Multi-Layer Switch](#)” on page 68.

In this example, the client-side HP EFS WAN Accelerator IP address **10.1.0.2**, its WAN router is **10.1.0.1**, and the server-side HP EFS WAN Accelerator, IP address is **10.2.0.2**.

#### Basic Steps (Client-Side)

Perform the following steps for the client-side HP EFS WAN Accelerator.

1. Configure the HP EFS WAN Accelerator in an in-path configuration. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
3. Navigate to the Setup: Optimization Service - General Settings page in the Management Console.
4. To enable external traffic redirection click **Enable In-Path Support, Enable L4/PBR/WCCP Support on Interface wan0\_0**, and **Enable Optimization on Interface inpath0\_0**.

**Figure 7-3.** Setup: Optimization Service - General Settings Page

The screenshot shows the 'Optimization Service - General Settings' page. The left sidebar has a dark grey background with white text. It lists several sections: Optimization Service (selected), General Settings (selected), In-Path Rules, Protocols (CIFS, MAPI, MS-SQL, Connection Pooling), Host Settings, Advanced Networking, Port Labels, Reports, Logging, Date & Time, Authentication, Licenses, Scheduled Jobs, Configuration Manager, Upgrade Software, Start/Stop Services, Reboot Appliance, and Shutdown Appliance. The main content area has a light grey background. It includes a note: 'Check and modify your base service settings.' Below this is the 'In-Path' section with the following checkboxes:

- Enable In-Path Support
- Reset Existing Client Connections on Start Up
- Enable L4/PBR/WCCP Support on Interface **wan0\_0**
- Enable Optimizations on Interface **inpath0\_0**
- Enable Optimizations on Interface **inpath0\_1**

Below this is the 'Out-of-Path (for server-side appliances only)' section with one checkbox:

- Enable Out-of-Path Support

At the bottom right are three buttons: 'Apply', 'Save', and 'Reset'.

5. Enable WCCP on your router.

**6.** Navigate to the Setup: Advanced Networking - WCCP Groups page.

**Figure 7-4.** Setup: Advanced Networking - WCCP Service Groups Page

**Advanced Networking - WCCP Service Groups**

Check and modify your WCCP v2 service groups. Click on a service group to modify its settings.

Service Group ID	Priority	Weight	Scheme
No WCCP service groups.			

Remove Selected Groups

**Add New Service Group:**

- Service Group ID: 90
- Router IP: 10.1.1.1
- Password:
- Confirm Password:
- Priority: 200
- Weight: 6
- Encapsulation Scheme: either

Add Group

**WCCP v2 Global Settings:**

- Enable WCCP v2 Support
- Multicast TTL: 1

Update Settings

Save Reset

7. Define the service group: specify the service group identification number, the router IP address, password, priority, weight, and encapsulation scheme, and optionally, global settings.
8. Click **Add Group** to display your new group in the Service Group list.
9. Under WCCP v2 Global Settings, click **Enable WCCP v2 Support**.
10. Click **Update Settings** to enable WCCP v2 support.
11. Double-click the new service group name to display the Setup: Service, WCCP Groups, Service Group page.
12. Define flags and ports; add additional routers for the service group.

**Figure 7-5.** Setup: Service, WCCP Groups Page

The screenshot shows the 'Advanced Services - WCCP Service Group: 90' configuration page. The left sidebar includes sections like Optimization Service, Host Settings, Advanced Networking (with WCCP Groups selected), Proxy File Service, Port Labels, Reports, Logging, Date & Time, Authentication, Licenses, Scheduled Jobs, Configuration Manager, Upgrade Software, Start/Stop Services, Reboot Appliance, and Shutdown Appliance.

**Group Settings:**

- Password:  (\*\*\*\*\*)
- Confirm Password:  (\*\*\*\*\*)
- Priority:  200
- Weight:  6
- Encapsulation Scheme:

**Flags:**

- Source IP Hash (checked)
- Destination IP Hash
- Source Port Hash
- Destination Port Hash

**Ports:**

- Ports Disabled
- Use Source Ports
- Use Destination Ports
- 

**Routers:**

- Router:**
- 10.1.1.1
- 
- Add Router IP:**

**Buttons:**

- 
-

**13.** Save and apply the new configuration in the Management Console.

**14.** Restart the HP EFS WAN Accelerator service in the Setup: Start/Stop Service page.

On the client-side, you add in-path rules to reach the out-of-path, server-side HP EFS WAN Accelerator. In this example you optimize ports **135**, **139**, **445**, **21**, and **80** to pass through all other traffic.

**To define in-path rules to reach the server-side appliance**

**15.** Navigate to the Setup: Optimization Service - In-Path Rules page in the Management Console.

**16.** Define a fixed-target rule to optimize traffic on the server-side HP EFS WAN Accelerator with port **135**.

**Figure 7-6.** Setup: Optimization Service - In-Path Rules Page

The screenshot shows the 'Optimization Service - In-Path Rules' page. On the left, a navigation menu includes 'In-Path Rules' under 'Optimization Service'. The main area shows a table of existing rules:

#	Type	Source	Destination	Port	Target	Port	Opt Policy	Neutral	VLAN
1	Fixed	All	All	All	10.0.0.3 10.0.0.2	135 135	Normal	Always	All
def	Auto	All	All	All	--	--	Normal	Always	All

Below the table are buttons for 'Remove Selected Rules', 'Move Rule', and 'Add New Rule'. The 'Add New Rule' section is expanded, showing fields for Type (Fixed-Target), Source Subnet (0.0.0.0/0), Destination Subnet (0.0.0.0/0), Port (all), Target Appliance IP (10.0.0.3), and Backup Appliance IP (10.0.0.2). Advanced options and additional options (Enable Computation of Neural Heuristics) are also present. At the bottom are 'Save' and 'Reset' buttons.

17. Repeat Step 4 for ports **139**, **445**, **21**, and **80**.
18. To pass through all other traffic, define a pass-through rule on the server-side HP EFS WAN Accelerator.

**Figure 7-7.** Setup: Optimization Service - In-Path Rules Page

The screenshot shows the 'Optimization Service - In-Path Rules' page. The left sidebar includes links for General Settings, In-Path Rules (selected), Protocol (CIFS, MAPI, MS-SQL, HSTCP), Connection Pooling, Host Settings, Advanced Networking, Proxy File Service, Port Labels, Reports, Logging, Date & Time, Authentication, Licenses, Scheduled Jobs, Configuration Manager, Upgrade Software, Start/Stop Services, Reboot Appliance, and Shutdown Appliance.

The main content area has a status bar: Status: Healthy [ config save required ] and Logged in as: admin [ logout ].

The 'In-Path Rules' table lists five rules:

#	Type	Source	Destination	Port	Target	Port	Opt Policy	Neural	VLAN
1	Fixed	All	All	All	10.0.0.0 10.0.0.1	80 80	Normal	Always	All
2	Fixed	All	All	All	10.0.0.8 10.0.0.9	21 21	Normal	Always	All
3	Fixed	All	All	All	10.0.0.6 10.0.0.7	445 445	Normal	Always	All
4	Fixed	All	All	All	10.0.0.4 10.0.0.5	139 139	Normal	Always	All
5	Fixed	All	All	All	10.0.0.3 10.0.0.2	135 135	Normal	Always	All
def	Auto	All	All	All	--	--	Normal	Always	All

Buttons below the table include Remove Selected Rules, Move Rule (with dropdowns for position), and Move Rule.

The 'Add New Rule' section contains fields for Type (Pass Through selected), Insert Rule At (start selected), Source Subnet (0.0.0.0/0), Destination Subnet (0.0.0.0/0), Port (all), Advanced Options (click to open), VLAN Tag ID (All dropdown), and an Add Rule button.

The 'Additional Options' section includes a checkbox for Enable Computation of Neural Heuristics and an Update Settings button.

At the bottom right are Save and Reset buttons.

19. Save and apply the new configuration in the Setup: Configuration Manager page.

20. Begin optimization. View performance reports and system logs in the Management Console.

## Basic Steps (Server-Side)

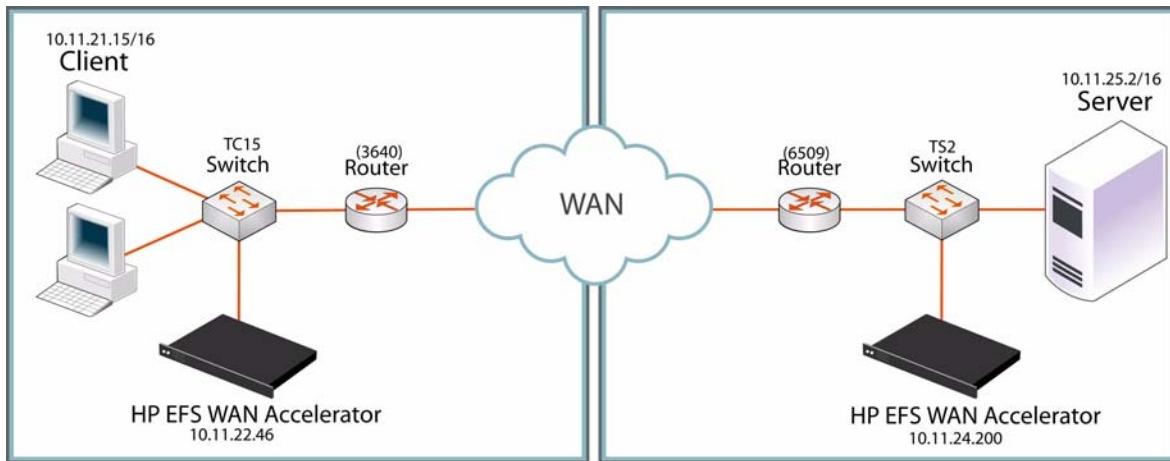
The server-side HP EFS WAN Accelerator is configured as an out-of-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

**IMPORTANT:** This is an example of one type of WCCP deployment. You can also have deployments with both HP EFS WAN Accelerators configured as in-path devices and WCCP configured on one of them. In this case, you would configure the server-side as an in-path device and you would not define fixed-target rules on the client-side. For detailed information, contact HP technical support at <http://www.hp.com>.

## Dual WCCP Deployment

The following section describes how to deploy two HP EFS WAN Accelerators that are physically out-of-path but virtually in-path so that traffic is directed to them using WCCP.

**Figure 7-8.** Dual WCCP Deployment



Traffic between client and server passes through the two routers. When each router is configured with a WCCP service group, all traffic is redirected to pass through the corresponding HP EFS WAN Accelerators as it transits the router, enabling the HP EFS WAN Accelerators to optimize the connections. Auto-discovery functions correctly—each HP EFS WAN Accelerator sends and receives traffic as if they were using an in-path configuration.

---

**IMPORTANT:** The HP EFS WAN Accelerators are connected using the WAN interface only.

---

WCCP uses a router identification number (ID) to announce the router to the HP EFS WAN Accelerators. The router ID is one of the interfaces IP addresses: the router ID is not guaranteed to be the address of the interface closest to the HP EFS WAN Accelerator.

The HP EFS WAN Accelerator must be able to route traffic back to the address that the router uses as the router ID. It is not sufficient to have the HP EFS WAN Accelerator know how to route to the client, server, and the server-side HP EFS WAN Accelerator; the HP EFS WAN Accelerator must know how to route traffic to the interface that the router takes its WCCP router ID from. The router ID can be changed by configuring a loop-back interface (**int loopback 0**) with a more suitable IP address.

The 6509 router uses hardware switching, if it can. It must be turned off using the **no mls ip** command on the interfaces which are enabled for WCCP.

### To configure the WCCP (3640) router

- At the system prompt, enter the following set of commands on the CISCO 3640 router:

```
version 12.3
service timestamps debug datetime localtime show-timezone
```

```
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname tr3640
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 errors
enable secret 5 $xxxxxxxx
!
clock timezone PST -8
clock summer-time PDT recurring
no aaa new-model
ip subnet-zero
ip wccp 90
!
ip cef
ip audit po max-events 100
no ftp-server write-enable
!
no crypto isakmp enable
!
interface FastEthernet0/0
 ip address 10.0.26.101 255.255.0.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clockrate 2000000
 no fair-queue
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
!
!Wan Interface
interface FastEthernet0/1.47
 encapsulation dot1Q 47
 ip address 172.20.240.17 255.255.255.252
 no ip redirects
 ip wccp 90 redirect in
 no cdp enable
!
!Client Interface
interface FastEthernet0/1.108
 encapsulation dot1Q 108
 ip address 10.11.21.100 0.0.0.255
 no ip redirects
 ip wccp 90 redirect in
 no cdp enable
!
!HP EFS WAN Accelerator Interface
interface FastEthernet0/1.132
 encapsulation dot1Q 132
 ip address 10.11.22.17 0.0.0.255
 no ip redirects
 no cdp enable
```

```

!
no ip http server
no ip http secure-server
no ip classless
ip route 10.11.24.0 0.0.0.255 172.20.240.18
ip route 10.11.25.0 0.0.0.255 172.20.240.18
!
no logging trap
!
control-plane
!
line con 0
line aux 0
line vty 0 4
exec-timeout 0 0
password 7 xxxxxxxx
login
transport input telnet
!
ntp server 10.0.0.2
!
end

```

### To configure the WCCP (6209) router

- At the system prompt, enter the following set of commands:

```

!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname cisco-6509
!
boot system flash sup-slot0:c6msfc2-jsv-mz.121-23.E.bin
boot system bootflash:c6msfc2-psv-mz.121-19.E1.bin
boot bootldr bootflash:c6msfc2-boot-mz.121-19.E1.bin
enable secret 5 $xxxxxxxxx
!
clock timezone PST -8
ip subnet-zero
ip wccp 91
!
interface Vlan1
  ip address 10.0.26.107 255.255.0.0
!
!Server Interface
interface Vlan54
  ip address 10.11.25.250 0.0.0.255
  no ip redirects
  ip wccp 91 redirect in
  no mls ip
  no mls ipx
  no cdp enable
!
!HP EFS WAN Accelerator Interface
interface Vlan55
  ip address 10.11.24.250 0.0.0.255
  no ip redirects
  no mls ip
  no mls ipx
  no cdp enable
!
!WAN Interface

```

```

interface Vlan63
  ip address 172.20.240.18 255.255.255.252
  no ip redirects
  ip wccp 91 redirect in
  no mls ip
  no mls ipx
  no cdp enable
!
ip classless
ip route 10.11.21.0 0.0.0.255 172.20.240.17
ip route 10.11.22.0 0.0.0.255 172.20.240.17
ip flow-export version 5
no ip http server
!
line con 0
  exec-timeout 0 0
line vty 0 4
  password 7 06541B2E5C175958
  login
!
end

```

**To configure the client-side HP EFS WAN Accelerator**

- At the system prompt, enter the following set of commands:

```

client-SH > enable
client-SH # configure terminal
client-SH (config) # interface in-path ip address 10.11.22.46 /16
client-SH (config) # in-path oop enable
client-SH (config) # in-path enable
client-SH (config) # wccp enable
client-SH (config) # wccp service-group 90 routers 10.11.22.17
flags,dst-ip-hash priority 200 weight 3 encapsulation either
client-SH (config) # write memory
client-SH (config) # restart

```

**To configure the server-side HP EFS WAN Accelerator**

At the system prompt, enter the following set of commands:

```

server-SH > enable
server-SH # configure terminal
server-SH (config) # interface in-path ip address 10.11.24.200 /16
server-SH (config) # in-path oop enable
server-SH (config) # in-path enable
server-SH (config) # wccp enable
server-SH (config) # wccp service-group 91 routers 10.11.24.250
flags,dst-ip-hash priority 200 weight 6 encapsulation either
server-SH (config) # write memory
server-SH (config) # restart

```

---

## Additional WCCP Features

This section describes the additional features for WCCP.

## Security

WCCP protocol messages can be authenticated between the router and the HP EFS WAN Accelerator using a password. The maximum password length is 8 characters.

**To set the password for WCCP**

1. On the router, at the system prompt, enter the following command:

```
Router(config)# ip wccp 90 password <your_password>
```

2. On the HP EFS WAN Accelerator, at the system prompt, enter the following command:

```
client-SH (config) # wccp service-group 90 routers 10.1.0.1 password  
<your_password>
```

---

**NOTE:** The same password must be set on the HP EFS WAN Accelerator and the router.

---

## Multicast

If you add multiple routers and HP EFS WAN Accelerators to a service group, you can configure them to exchange WCCP protocol messages through a multicast group.

Configuring a multicast group is advantageous because if a new router is added, it does not need to be explicitly added on each HP EFS WAN Accelerator.

### To configure multicast groups on your router

- On your router, at the system prompt, enter the following set of commands:

```
Router> enable  
Router# configure terminal  
Router(config)# ip wccp version 2  
Router(config)# ip wccp 90 group-address 224.0.0.3  
Router(config)# interface fastEthernet 0/0  
Router(config-if)# ip wccp 90 redirect in  
Router(config-if)# ip wccp 90 group-listen  
Router(config-if)# end  
Router#
```

---

**TIP:** Enter configuration commands, one per line. End each command with CTRL-Z.

---

### To configure multicast groups on the HP EFS WAN Accelerator

- On the client-side HP EFS WAN Accelerator, at the system prompt, enter the following set of commands:

```
client-SH > enable  
client-SH # configure terminal  
client-SH (config) # wccp enable  
client-SH (config) # wccp mcast-ttl 10  
client-SH (config) # wccp service-group 90 routers 224.0.0.3  
client-SH (config) # write memory  
client-SH (config) # exit
```

## TCP Port Redirection

By default, all TCP ports are redirected, but the HP EFS WAN Accelerator can be configured to tell the router to redirect only certain TCP source or destination ports. A maximum of 7 ports can be specified per service groups.

---

**NOTE:** You do not need to configure source and destination ports on the router.

---

### To configure TCP port redirection

- On the client-side HP EFS WAN Accelerator, at the system prompt, enter the following command:

```
client-SH (config) # wccp service-group 90 routers 10.1.0.1 flags ports-
destination ports 135,139,445,21,80
```

## Specific Traffic Redirection

### To configure specific traffic redirection on the router

If redirection is based on traffic characteristics other than ports, Access Control Lists (ACLs) on the router can define what traffic is redirected.

For example, if you only want the traffic destined for IP address **10.2.0.0/16** to be redirected to the HP EFS WAN Accelerator, you would configure the router in the following manner.

- On the router, enter the following set of commands:

```
Router> enable
Router# configure terminal
Router(config)# ip wccp version 2
Router(config)# access-list 101 permit tcp any 10.2.0.0 255.255.0.0
Router(config)# ip wccp 90 redirect-list 101
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip wccp 90 redirect in
Router(config-if)# end
Router#
```

---

**TIP:** Enter configuration commands, one per line. End each command with CTRL-Z.

---

## Load Balancing

### To change the hashing scheme and assign a weight

You can load-balance using WCCP. Traffic is redirected based on a hashing scheme and the weight of the HP EFS WAN Accelerators. You can hash on a combination of the source IP address, destination IP address, source port, or destination port. The default weight is based on the HP EFS WAN Accelerator model (for example, for the Model 5000 the weight would be 5000). You can modify the default weight.

For example, to configure load balancing, you change the hashing scheme to hash on a destination IP and port and specify a weight on the HP EFS WAN Accelerator. (You do not need to configure the router.)

1. On the client-side HP EFS WAN Accelerator, enter the following command:

```
client-SH (config) # wccp service-group 90 routers 10.1.0.1 flags dst-
ip-hash,dst-port-hash
```

2. To change the weight on the client-side HP EFS WAN Accelerator, enter the following command:

```
client-SH (config) # wccp service-group 90 routers 10.1.0.1 weight 20
```

## Failover Support

You can also provide failover support using WCCP. In a failover configuration, the HP EFS WAN Accelerators periodically announce themselves to the routers. If an HP EFS WAN Accelerator fails, traffic is redirected to the working HP EFS WAN Accelerators.

For example, instead of load balancing traffic between two HP EFS WAN Accelerators, you might want traffic to go to only one HP EFS WAN Accelerator and to failover to the other HP EFS WAN Accelerator if the first one fails.

To configure failover support, you simply define the weight to be **0** on the backup HP EFS WAN Accelerator. For detailed information, see “[WCCP CLI Commands](#)” on page 66.

---

## Troubleshooting

You can check your WCCP configuration on the router and the HP EFS WAN Accelerator.

### To check the router configuration

- On the router, at the system prompt, enter the following set of commands:

```
Router>en
Router#show ip wccp
Router#show ip wccp 90 detail
Router#show ip wccp 90 view
```

You can trace WCCP packets and events on the router.

### To trace WCCP packets and events on the router

- On the router, at the system prompt, enter the following set of commands:

```
Router>en
Router#debug ip wccp events
WCCP events debugging is on
Router#debug ip wccp packets
WCCP packet info debugging is on
Router#term mon
```

## CHAPTER 8

# Proxy File Service Deployments

## In This Chapter

This chapter describes Proxy File Service (PFS) and provides the basic steps for configuring PFS. This chapter includes the following sections:

- ◆ “[Introduction to PFS](#),” next
- ◆ “[PFS Terms](#)” on page 84
- ◆ “[How Does PFS Work?](#)” on page 86
- ◆ “[Configuring PFS Using the Management Console](#)” on page 89

This chapter assumes that you are familiar with the installation and configuration process for the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

This chapter also assumes you are familiar with the HP EFS WAN Accelerator Management Console (Management Console). For detailed information about the Management Console and how to use it, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

---

**NOTE:** The Setup: Proxy File Service (PFS) - Configuration page only appears if you are running an HP EFS WAN Accelerator, Model DL320-510, DL320-1010, DL320-2010, DL320-520, DL320-1020, DL320-2020, DL380-3010, or DL380-5010. These models have the necessary disk capacity to perform PFS.

---

## Introduction to PFS

PFS is an optional integrated virtual file server that allows you to store copies of files on the HP EFS WAN Accelerator with Windows file access, creating several options for transmitting data between remote offices and centralized locations with improved performance and functions. Data is configured into file shares by PFS; and the shares are periodically synchronized (updated) transparently in the background, over the optimized connection of the HP EFS WAN Accelerator. PFS leverages the integrated disk capacity of the HP EFS WAN Accelerator to store file-based data in a format that allows it to be retrieved by Network Attached Storage (NAS) clients.

PFS runs in concert with the HP EFS Remote Copy Utility (HP EFS RCU). The HP EFS RCU must be installed on the origin server or on a separate Windows host with write-access to the data utilized by PFS. For detailed information, see the *HP Enterprise File Services Remote Copy Utility Reference Manual*.

PFS provides:

- ◆ **LAN access to data residing across the WAN.** File access performance is improved between central and remote locations. PFS creates an integrated file-server, enabling clients to access data directly from the PFS on the LAN as opposed to the WAN. Transparently in the background, data on the PFS is synchronized with data from the origin file server over the WAN.
- ◆ **Continuous access to files in the event of WAN disruption.** PFS provides support for disconnected operations. In the event of a network disruption that prevents access over the WAN to the origin server, files can still be accessed on the local HP EFS WAN Accelerator.
- ◆ **Simplify Branch Infrastructure and Backup Architectures.** PFS consolidates file servers and local tape backup from the branch into the data center. PFS enables a reduction in number and size of backup windows running in complex backup architectures.

---

## PFS Terms

The following terms are used to describe processes and devices in PFS.

---

Proxy File Service Term	Description
Proxy File Server	A virtual file server resident on the HP EFS WAN Accelerator, providing Windows file access (with Access Control Lists (ACLs)) capability at a branch office on the LAN network, populated over an optimized WAN connection with data from the origin server.
Origin Server	The server located in the data center which hosts the origin data volumes.
Domain Name	The domain to which you want to make the proxy file server a member. Typically, this is the same domain as your company's domain.

Proxy File Service Term	Description
Domain Controller (DC)	Specifies the domain controller name, the host that provides user login service in the domain. (Typically, with Windows 2000 Active Directory Service domains, given a domain name, the system automatically retrieves the domain controller name.)
Share	The data volume exported from the origin server to the remote HP EFS WAN Accelerator.
Local Name	The name that you assign to a share on the HP EFS WAN Accelerator, this is the name by which users identify and map a share.
Remote Path	The path to the data on the origin server or the Universal Naming Convention (UNC) path of a share to which you want to make available to PFS.
RCU Server	The name of the Windows server where the HP EFS Remote Copy Utility (HP EFS RCU) is running. The RCU server may be the same as the origin server.
Share Synchronization	Synchronization runs periodically in the background, ensuring that the data on the proxy file server is synchronized with the origin server. You have the HP EFS WAN Accelerator refresh the data automatically by setting the frequency, in seconds; or manually at anytime.

## PFS Operating Modes

Each individual file share on the HP EFS WAN Accelerator is configured in one of the following operating modes:

- ◆ **Broadcast Mode.** Provides branch-office HP EFS WAN Accelerators with local read-only copies of data stored on the origin server. CIFS clients who map a **Broadcast** mode file share on the HP EFS WAN Accelerator cannot make changes to the files in that file share. The data is updated periodically on the HP EFS WAN Accelerator with the data from the origin server. You specify the frequency of updates (synchronization) when you configure a share.
- ◆ **Local Mode.** Provides read-write access to a given file share hosted on the branch-office HP EFS WAN Accelerator. CIFS clients mapping a **Local** mode file share have read-write access to that share. Changes made to the share are sent back to the origin server. For any remote path, there can exist only one local share on any HP EFS WAN Accelerator, this prevents conflicting data from being written to the same path.

---

**NOTE:** In **Local Mode**, the HP EFS WAN Accelerator copy of the data is the master copy, do not make changes to the shared files on the origin server directory while in **Local** mode. Changes are propagated from the HP EFS WAN Accelerator to the origin server.

---

---

**NOTE:** When you configure a share, a text file (**.\_rbt\_share\_lock.txt**), is created on the origin server that keeps track of which HP EFS WAN Accelerator owns the share. Do not remove this file. If you remove the **.\_rbt\_share\_lock.txt** file on the origin file server, PFS will not function properly.

---

- ◆ **Stand-Alone Mode.** Provides the client read-write access to data on a remote HP EFS WAN Accelerator. For example, if you want to load temporary data from a remote client to the remote HP EFS WAN Accelerator that does not need to be backed up at a data center, you can create a share in **Stand-Alone** without a remote path. A **Stand-Alone** share with a remote path is initially populated with data from the origin server after which changes and/or new data created on the share are not sent back to the origin server.
- ◆ **Global Mode.** HP EFS WAN Accelerator optimization without PFS enabled.

---

## How Does PFS Work?

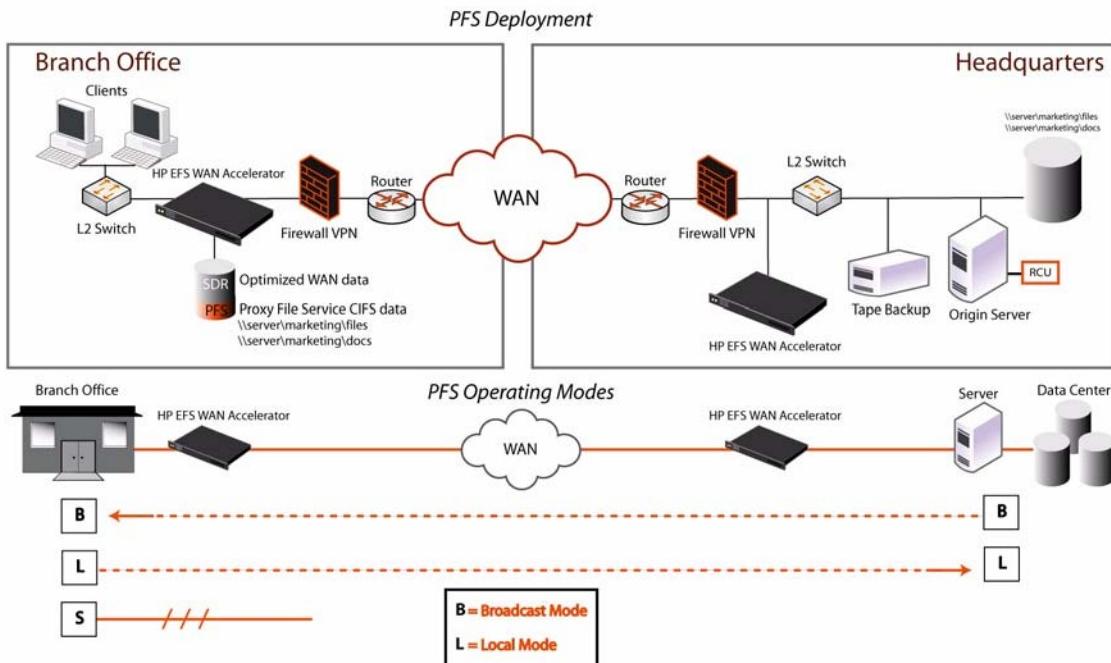
To synchronize the data volumes, the HP EFS WAN Accelerator communicates to the HP EFS RCU running on the origin server. If the origin server is a non-Windows file server and cannot run the HP EFS RCU, then the HP EFS RCU can be run on a Windows server with write-access, to the origin server.

PFS provides Windows file service in the HP EFS WAN Accelerator at a remote site. The HP EFS WAN Accelerator is configured as a Domain Member Server. Data volumes at the data center are configured explicitly on the proxy file server and are served locally by the HP EFS WAN Accelerator. As part of the configuration, the data volume including the Access Control Lists (ACLs) from the origin server are copied on to the HP EFS WAN Accelerator. PFS allocates a portion of the HP EFS WAN Accelerator data store for users to access as a network file system.

PFS in the HP EFS WAN Accelerator allows a Domain Controller (DC) to authenticate users accessing its file shares. The DC can be located at the remote site or over the WAN at the main data center. The HP EFS WAN Accelerator must be configured as a Member Server in the Windows 2000, or later, Active Directory Services (ADS) domain. Domain users are allowed to access the PFS shares based on the access permission settings provided for each user.

The proxy file server can export data volumes in local mode, broadcast mode, and stand-alone mode. After the HP EFS WAN Accelerator receives the initial copy of the data and ACLs, the shares can then be made available to local clients. The shares on the HP EFS WAN Accelerator will periodically be synchronized with the origin server at specified intervals, or manually by the system administrator. The HP EFS WAN Accelerator uses Scalable Data Referencing (SDR) during the synchronization process which optimizes the traffic across the WAN.

**Figure 8-1. PFS Deployment**



## When to Use PFS

PFS can be configured with any number of file shares in different modes. Shares are configured into different operating modes based on the use of your data:

- ◆ For environments seeking to broadcast a set of read-only files to many users at different sites. **Broadcast Mode** quickly transmits a read-only copy of the files from the origin server to your remote offices.
- ◆ For environments that need to efficiently and transparently copy data created at a remote site to a central data center, perhaps where tape archival resources are available to backup the data. **Local Mode** enables read-write access at remote offices to update files on the origin file server.
- ◆ For network environments where it is more effective to maintain a separate copy of files that are accessed locally by the clients at the remote site. In **Stand-Alone Mode**, create a proxy file server at a remote office using the remote office HP EFS WAN Accelerator, creating extra storage space.

If any of the above advantages can benefit your environment, then enabling PFS in the HP EFS WAN Accelerator is appropriate.

## When to use Global Mode

Deploying the HP EFS WAN Accelerator without PFS is considered *global mode*. In global mode, the HP EFS WAN Accelerator performs its standard optimization of accessing data over the WAN.

Evaluate whether PFS is suitable for your network needs:

- ◆ **Pre-Identification of PFS files.** PFS requires that files accessed over the WAN must be identified in advance. If the data set accessed by the remote users is larger than the specified capacity of your model or if it cannot be identified in advance, then you should have end-users access the origin server directly through the HP EFS WAN Accelerator without PFS (global mode).
- ◆ **Concurrent Read-Write Data Access from Multiple Sites.** In a network environment where users from multiple branch offices update a common set of centralized files and records over the WAN, the HP EFS WAN Accelerator *without* PFS is the most appropriate solution because file locking is directed between the client and the server. The HP EFS WAN Accelerator always consults the origin server in response to a client request, it never provides a proxy response or data from its data store without consulting the origin server.

PFS requires an HP EFS WAN Accelerator Model DL320-520, DL320-1020, DL320-2020, DL380-3010, or DL380-5010. These models have extra disk capacity that is utilized when PFS is enabled.

## Configuration Checklist for PFS

Before you enable PFS make sure you:

- ◆ configure the HP EFS WAN Accelerator to use Network Time Protocol (NTP) to synchronize the time. For detailed information about setting the date and time in the HP EFS WAN Accelerator, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
- ◆ configure the DNS server correctly. The configured DNS server must be the same DNS server to which all the Windows client machines point to.
- ◆ have a fully qualified domain name for which PFS will be configured. This domain name must be the domain name for which all the Windows desk-top machines are configured.
- ◆ configure the HP EFS WAN Accelerator as a member server in the Windows 2000 domain so that the HP EFS WAN Accelerator can access the domain controller to authenticate the users accessing its file shares. In order to perform this operation, a Windows domain account is required with the privileges to perform a **join domain** operation.
- ◆ you must make sure that the owner of the remote path is a **domain account** and not a local account.
- ◆ install and start the HP EFS Remote Copy Utility (HP EFS RCU) on the origin server. You can install the RCU on the origin server or on a separate Windows host with write access to the data utilized by PFS. The RCU is available for download from the HP support site located at <http://www.hp.com>. For detailed information, see the *HP Enterprise File Services Remote Copy Utility Reference Manual*.

## Configuring PFS Using the Management Console

The following sections provide the basic steps for joining the domain for PFS, and configuring PFS shares for Broadcast, Local, or Stand-Alone mode using the Management Console.

### To join a domain for PFS

1. Install and start the HP EFS RCU on the HP EFS RCU server, which by default listens on port 8777. The RCU service must be started with a domain account that has write access to the share on the origin server.
2. Configure the HP EFS WAN Accelerator as an in-path device. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

---

**IMPORTANT:** HP EFS RCU traffic from the HP EFS WAN Accelerator originates through the Primary Interface. To ensure proper optimization of HP EFS RCU traffic, make sure traffic from your Primary interface goes through the same switch as your LAN interface. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

---

3. Connect to the Management Console. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.
4. Navigate to the Setup: Proxy File Service (PFS) - Configuration page. You will need to join a domain the first time you configure PFS.

**Figure 8-2.** Setup: Proxy File Service (PFS) - Configuration Page.

The screenshot shows the 'Proxy File Service (PFS) - Configuration' page. At the top, there's a navigation bar with links for Home, Setup, Reports, Logging, Help, and a status indicator 'Status: Healthy'. To the right of the status is a message 'Logged in as: admin [ logout ]'. Below the navigation is a sidebar with a dark background containing a list of setup categories:

- Optimization Service
- Host Settings
- Advanced Networking
- Proxy File Service** (selected)
  - Configuration
  - Shares
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs

**Proxy File Service Configuration**

Fully-Qualified Domain Name/Realm:

Domain Controller Name (optional):

Primary DNS IP:

Domain Admin Login:

Domain Admin Password:

**Security Signature Settings**

Security Signature:

**Idle Connection Timeout**

Idle Connection Timeout:  mins

**Local Administrator Settings**

Local Admin Password:

Confirm:

5. Under Proxy File Service Configuration, enter the domain name in the **Fully-Qualified Domain Name/Realm** text box.
6. Optionally, enter the domain controller name in the **Domain Controller Name** text box.

---

**NOTE:** The **Primary DNS IP** displays the primary DNS IP as an active link. To change the primary DNS IP, click on this link to be taken to the Setup: Host Settings - DNS Settings page. For more information on DNS Settings, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

---

7. Enter the domain administrator login, and password in the **Domain Admin Login** and **Domain Admin Password** text boxes.

8. Click **Update PFS Configuration**. You are notified if the HP EFS WAN Accelerator successfully joined the domain.

9. Under Enable/Disable Proxy File Service, click **Enable PFS** to enable PFS.

10. Under Security Signature Settings, select **Enabled**, **Disabled**, or **Required** from the **Security Signature** drop-down list and click **Update Security Signature Settings**.

<b>Disabled</b>	This is the default setting. In this setting, PFS does not support clients with security signatures set to <i>required</i> .
<b>Enabled</b>	This setting supports any type of security signature setting requested by the client machine.
<b>Required</b>	In this setting, PFS only supports clients with security signatures set to enabled.

11. Under Idle Connection Timeout, type a timeout value in minutes in the text box and click **Update the Connection Timeout**. If there is no client (read or write) activity

12. Under Local Administrator Settings, type the local administrator password in the **Local Admin Password** text box. You must use the correct syntax for the administrator login name (for example: **admin\_user@parent\_realm**) even if you belong to a subdomain.

13. Retype the local administrator password in the **Confirm** text box and click **Update Administrator Settings**. The local administrator account can be used to manage PFS files when the WAN is down.

14. Click **Save** to write your settings to memory.

15. Navigate to the Setup: Start/Stop Service page.

16. Under Optimization, click **Restart Service** to restart the HP EFS WAN Accelerator service.

17. Under PFS, click **Start Service** to start PFS.

---

**TIP:** Select **Automatic**, or **Manual** from the **Startup** drop-down list in the Setup: Start/Stop Services page to specify whether you want the service to start automatically on system reboot or manually.

---

- 18.** Navigate to the Setup: Configuration Manager page and save your changes to memory.

After you have setup the PFS domain, you can configure your shares.

### To add a share for PFS

1. Navigate to the Setup: Proxy File Service (PFS) - Shares page.

**Figure 8-3.** Setup: Proxy File Service - Shares Page

The screenshot shows the 'Proxy File Service - Shares' page. At the top, there's a navigation bar with 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The status is 'Healthy [ config save required ]' and the user is logged in as 'admin [ logout ]'. On the left, a sidebar menu includes 'Optimization Service', 'Host Settings', 'Advanced Networking', 'Proxy File Service' (selected), 'Shares' (selected), 'Port Labels', 'Reports', 'Logging', 'Date & Time', 'Authentication', 'Licenses', 'Scheduled Jobs', 'Configuration Manager (1)', 'Upgrade Software', 'Start/Stop Services', 'Reboot Appliance', and 'Shutdown Appliance'. The main area displays a table of shares:

Local Name	Description	Mode	Sharing	Syncing	Actions	Status
field_kit	dfs1 : \\(townsend\marketing\field_kit	Local			Sync, Verify	Share idle
marketing	townsend : c:\shares\marketing	Local	✓	✓	Sync, Verify	Share idle
pfs2	dfs1 : c:\data\pfs-2	Broadcast	✓	✓	Sync, Verify	Share idle
pfs	dfs1 : c:\data\pfs	Local	✓	✓	Sync, Verify	Share idle
pfsB	dfs1 : c:\data\pfs-b	Broadcast	✓	✓	Sync, Verify	Share idle
unc-test-local	dfs1 : \\(treetop\pfstest	Local	✓	✓	Sync, Verify	Share idle
unc-test1	dfs1 : \\(treetop\pfstest	Broadcast	✓	✓	Sync, Verify	Share idle

Buttons at the bottom include 'Remove Selected Shares' and 'Update Shares'. Below the table is a modal dialog titled 'Add New Share:' with fields for Local Name, Mode (Broadcast selected), Remote Path, Server Name, Port, Sync Frequency (3600 seconds), and Comment. Buttons in the modal are 'Add Share', 'Save', 'Manual Sync', 'Verify', and 'Cancel'.

2. Under Add New Share, specify the local name for the share in the **Local Name** text box. This is the name to be used by clients for mapping.
3. Select **Broadcast**, **Local**, or **StandAlone** from the **Mode** drop-down list.

Mode	Description
Broadcast	In Broadcast mode, the share originates on the origin server and a read-only copy is available as a share on the branch office HP EFS WAN Accelerator. The data is updated periodically on the HP EFS WAN Accelerator with the data from the origin server. You specify the frequency of updates (synchronization) when you configure a share.
Local	<p>In Local mode, after the HP EFS WAN Accelerator receives the initial copy, new data generated by clients is periodically synchronized to the origin server. The folder on the origin server essentially becomes a back-up folder of the share on the HP EFS WAN Accelerator. Users must not directly write to this folder on the origin server.</p> <p>For Local mode, make sure that the folder on the origin server is either not shared or is shared as a read-only folder.</p>
StandAlone	<p><b>CAUTION:</b> In Local Mode, the HP EFS WAN Accelerator copy of the data is the master copy, do not make changes to the shared files from the origin server while in Local mode. Changes are propagated from the remote office hosting the share to the origin server.</p>

- Type the remote path for the share in the **Remote Path** text box.

**TIP:** if the origin server is not the HP EFS RCU server, you specify the remote path using the Uniform Naming Convention (UNC) for the mapped drive. For example, `\<origin-file-server>\<local-name>`. If the origin server is the same as the HP EFS RCU server then you must type its full path including the drive letter, for example `C:\data`.

- Type the HP EFS RCU server name and port in the **Server Name** and **Port** text boxes.
- Type frequency of updates (synchronization) in seconds, in the **Sync Frequency** text box.
- Optionally, type a comment that describes the share in the **Comment** text box.
- Click **Add Share** to add the share to the Shares list.
- Click **Save** to write your settings to memory.

## To synchronize and initialize a share

1. Navigate to the Setup: Proxy File Service - Shares page.
2. In the Shares list check the **Sync** check box and click **Update Shares**. This action downloads the initial copy of the share from the origin server to the HP EFS WAN Accelerator and configures the share for automatic synchronization.

**Figure 8-4.** Synchronizing, Initializing, and Accessing Shares

The screenshot shows the 'Proxy File Service - Shares' page. The left sidebar includes sections for Optimization Service, Host Settings, Advanced Networking, Proxy File Service (selected), Port Labels, Reports, Logging, Date & Time, Authentication, Licenses, Scheduled Jobs, Configuration Manager, Upgrade Software, Start/Stop Services, Reboot Appliance, and Shutdown Appliance. The main area displays a table of shares:

Local Name	Description	Mode	Sharing	Syncing	Actions	Status
field_kit	dfs1 : \\townsend\marketing\field_kit	Local	<input type="checkbox"/>	<input type="checkbox"/>		Share idle
marketing	townsend : c:\shares\marketing	Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Share idle
pfs2	dfs1 : c:\data\pfs-2	Broadcast	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Share idle
pfs	dfs1 : c:\data\pfs	Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Share idle
pfsB	dfs1 : c:\data\pfs-b	Broadcast	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Share idle
unc-test-local	dfs1 : \\treetop\pfstest	Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Share idle
unc-test1	dfs1 : \\treetop\pfstest	Broadcast	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Share idle

Buttons at the bottom include 'Remove Selected Shares' and 'Update Shares'. Below the table are three buttons: 'Manual Sync' (radio button), 'Verify' (checkmark icon), and 'Cancel' (cross icon). The 'Add New Share' dialog box is open, containing fields for Local Name, Mode (Broadcast selected), Remote Path, Server Name, Port (8777), Sync Frequency (3600 seconds), and Comment. A 'Save' button is located at the bottom right of the dialog.

## To map a share

3. Click the **Sharing** check box and click **Update Shares** to make the share available to clients for mapping. End users access the configured shares by mapping, for example, \\HP EFS WAN Accelerator\share1.

4. Click **Save** to write your settings to memory.
5. Navigate to the Setup - Configuration Manager page to apply and save the new configuration to memory. If you do not save your configuration changes to memory, your defined proxy file shares will become *orphaned*. Orphaned shares must be reconfigured to be synchronized.

---

**TIP:** You may choose at any time to click the **Manual Sync** button to manually synchronize a share. Click the **Verify** button to verify your shares, this will generate a list of the differences between the shares on the HP EFS WAN Accelerator and the origin server. Click the **Cancel** button to cancel your actions.

---



---

**TIP:** To remove a proxy file share, click the check box next to the name and click **Remove Selected Shares**. Click **Save** to write your settings to memory.

---



---

**CAUTION:** Removing a share means deleting the files of the share from the HP EFS WAN Accelerator. You must first disable **Syncing** to delete a share.

---

### To modify share information

1. Navigate to the Setup: Proxy File Service - Shares page.
2. In the Shares list, click the magnifying glass next to the Share name that you want to modify to display the Shares Detailed Settings page.

**Figure 8-5. Shares Detailed Settings Page**

The screenshot shows the 'Shares Detailed Settings' page. The left sidebar has a 'Proxy File Service' menu item under 'Shares'. The main form has the following fields:

- Local Name:** june-townsend
- Remote Path:** c:\june
- Server Name:** townsend
- Mode:** Local
- Sync Frequency:** 60 seconds
- Port:** 8777
- Sharing:**
- Syncing:**
- Comments:**
- Actions:**

At the bottom right are 'Update Share' and 'Save' buttons.

3. Modify your values and click **Update Share**.
4. Click **Save** to write your settings to memory.

**To view share status details**

1. Click **Jump to Share Status** to navigate to the Setup: Proxy File Service - Shares page.

**Figure 8-6.** Viewing the Share Status Page

The screenshot shows a web-based management interface for a proxy file service. On the left is a dark sidebar menu with several sections: Performance, Network, Health, Proxy File Service (with a 'Share Status' link), Export, and Diagnostic. The 'Share Status' link under 'Proxy File Service' is highlighted. The main content area has a title 'Share Status' and a note: 'The following is a list of Proxy Filer Service Shares.' It includes a refresh button and a link to 'Jump to Share Configuration'. A table lists 12 shares with columns for Local Name, Sharing, Syncing, Status, Last Synced, and Last Sync Status. Most shares are healthy (green checkmarks), except for one ('field\_kit') which is marked as 'Share idle' with red 'X' icons in the Sharing and Syncing columns.

Local Name	Sharing	Syncing	Status	Last Synced	Last Sync Status
field_kit	X	X	Share idle	Tue Nov 8 13:13:44 2005	X
marketing-mint	✓	✓	Share idle	Tue Jan 10 16:15:22 2006	✓
test-mint-local	✓	✓	Share idle	Tue Jan 10 16:18:01 2006	✓
marketing-test1	✓	✓	Share idle	Tue Jan 10 16:17:54 2006	✓
unc-test-townsend	✓	✓	Share idle	Tue Jan 10 16:17:31 2006	✓
marketing	✓	✓	Share idle	Tue Jan 10 16:17:59 2006	✓
unc-test-mp3	✓	✓	Share idle	Tue Jan 10 16:14:26 2006	✓
pfs2	✓	✓	Share idle	Tue Jan 10 16:13:47 2006	✓
pfs	✓	✓	Share idle	Tue Jan 10 16:17:06 2006	✓
pfs_B	✓	✓	Share idle	Tue Jan 10 16:14:47 2006	✓
unc-test-local	✓	✓	Share idle	Tue Jan 10 16:17:26 2006	✓
unc-test1	✓	✓	Share idle	Tue Jan 10 16:03:12 2006	✓

## CHAPTER 9

# RADIUS and TACACS+ Authentication

## In This Chapter

This chapter describes how to configure Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) authentication for the HP EFS WAN Accelerator. It contains the following sections:

- ◆ “Introduction to Authentication,” next
- ◆ “Configuring a RADIUS Server with FreeRADIUS” on page 98
- ◆ “Configuring a TACACS+ Server with Free TACACS+” on page 100
- ◆ “Configuring RADIUS Authentication in the HP EFS WAN Accelerator” on page 101
- ◆ “Configuring TACACS+ Authentication in the HP EFS WAN Accelerator” on page 103

---

## Introduction to Authentication

The HP EFS WAN Accelerator can use a RADIUS or TACACS+ authentication system for logging in administrative and monitor users. The following methods for user authentication are provided with the HP EFS WAN Accelerator:

- ◆ local
- ◆ radius
- ◆ tacacs+

The order in which authentication is attempted is based on the order specified in the Authentication, Authorization, Accounting (AAA) method list. The **local** value must always be specified in the method list.

The authentication methods list provides backup methods if a method fails to authenticate a user. Failure is defined as no response for the method. If a deny is received from the method being tried, no other methods are attempted.

The HP EFS WAN Accelerator does not have the ability to set a per interface authentication policy. The same authentication method list is used for all interfaces (that is, default). You cannot configure authentication methods with subsets of the RADIUS or TACACS+ servers specified (that is, there are no server groups).

The following CLI commands are available for RADIUS and TACACS+ authentication:

- ◆ Authentication
  - ◆ **aaa authentication login default**
  - ◆ **aaa authorization map default-user**
  - ◆ **aaa authorization map order**
  - ◆ **show authentication method**
- ◆ RADIUS Configuration
  - ◆ **radius-server host**
  - ◆ **radius-server key**
  - ◆ **radius-server retransmit**
  - ◆ **radius-server timeout**
- ◆ TACACS+ Configuration
  - ◆ **tacacs-server host**
  - ◆ **tacacs-server key**
  - ◆ **tacacs-server retransmit**
  - ◆ **tacacs-server timeout**
  - ◆ **show tacacs**
- ◆ User Accounts
  - ◆ **username privilege**
  - ◆ **username nopassword**
  - ◆ **username password**
  - ◆ **username password 0**
  - ◆ **username password 7**
  - ◆ **username password cleartext**
  - ◆ **username password encrypted**
  - ◆ **username disable**

---

## Configuring a RADIUS Server with FreeRADIUS

You can, on a per user basis, specify a different local account mapping by using a vendor specific attribute. This section describes how to configure the FreeRADIUS server to return an attribute (which specifies the local user account as an ASCII string). The file paths are the default values. If the RADIUS server installation has been customized, the paths might differ.

The directory **/usr/local/share/freeradius** is where the dictionary files are stored. This is where RADIUS attributes can be defined. Assuming the vendor does not have established dictionary file in the FreeRADIUS distribution, you begin the process by creating a file called: **dictionary.<vendor>**.

The contents of the **dictionary.<vendor>** file define a vendor identifier (which ought to be the Structure of Management Information (SMI) Network Management Private Enterprise Code of the Vendor), and the definitions for any vendor specific attributes.

In the following example, the Vendor Enterprise Number for HP is **17613** and the Enterprise Local User Name Attribute is **1**. These numbers specify that a given user is an **admin** or **monitor** user in the RADIUS server (instead of using the HP EFS WAN Accelerators default for users not named **admin** and **monitor**).

These instruction assume you are running FreeRADIUS, v.1.0, which is available from <http://www.freeradius.org>.

#### To install FreeRADIUS on a Linux computer

1. Download FreeRadius from <http://www.freeradius.org>.

2. At your system prompt, enter the following set of commands:

```
>tar xvzf freeradius-$VERSION.tar.gz
>cd freeradius-$VERSION
>./configure
>make
>make install #as root
```

#### To add acceptance requests on the RADIUS server

1. In a text editor, open the **/usr/local/etc/raddb/clients.conf** file.

2. To create the key for the RADIUS server, add the following text to the **clients.conf** file:

```
client 10.0.0.0/16 {
    secret = testradius
    shortname = main-network
    nastype = other
}
```

The secret you specify here must also be specified in the HP EFS WAN Accelerator when you set up RADIUS server support. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

3. In a text editor, create a **/usr/local/share/freeradius/dictionary.rbt** file for HP.

4. Add the following text to the **dictionary.rbt** file.

VENDOR	RBT	17163
ATTRIBUTE	Local-User	1 string RBT

5. Add the following line to the **/usr/local/share/freeradius/dictionary**:

```
$INCLUDE dictionary.rbt
```

6. Add users to the Radius server by editing the **/usr/local/etc/raddb/users** file. For example:

```
"admin"          Auth-Type := Local, User-Password == "radadmin"
                  Reply-Message = "Hello, %u"
```

```

"monitor"      Auth-Type := Local, User-Password == "radmonitor"
                Reply-Message = "Hello, %u"
"raduser"       Auth-Type := Local, User-Password == "radpass"
                Local-User = "monitor", Reply-Message = "Hello, %u"

```

7. Start the server using **/usr/local/sbin/radiusd**. Use the **-X** option if you want to debug the server.

**NOTE:** The **raduser** is the monitor user as specified by Local, User-Password.

## Configuring a TACACS+ Server with Free TACACS+

The following section assumes you are running the TACACS+ authentication system.

The TACACS+ Local User Service is **rbt-exec**. The Local User Name Attribute is **local-user-name**. This attribute controls whether a user who is not named **admin** or **monitor** is an administrator or monitor user (instead of using the HP EFS WAN Accelerator default value). For the HP EFS WAN Accelerator, the users listed in the TACACS+ server must have Password Authentication Protocol (PAP) authentication enabled.

The following procedures install the free TACACS+ server on a Linux computer. Cisco Secure can be used as a TACACS+ server.

### To download TACACS+

1. Download TACACS+ from:  
[http://www.gazi.edu.tr/tacacs/get.php?src=tac\\_plus\\_v9a.tar.gz](http://www.gazi.edu.tr/tacacs/get.php?src=tac_plus_v9a.tar.gz).
2. At your system prompt, enter the following set of commands:

```
>tar xvzf tac_plus_v9a.tar.gz
>cd tac_plus_v9a
>./configure
```

3. In a text editor, open the **Makefile** and uncomment the **OS=-DLINUX** line (or other lines appropriate for the operating system of the host).
4. On Linux, in a text editor open the **tac\_plus.h** file and uncomment the **#define CONST\_SYSERRLIST** line.

5. At the system prompt, enter:

```
>make tac_plus
```

6. As the root user, enter the following command:

```
>make install
```

7. Add users to the TACACS server by editing the **/usr/local/etc/tac\_plus.conf** file.  
For example:

```
key = testtacacs
```

```

user = admin {
    pap = cleartext "tacadmin"
user = monitor {
    pap = cleartext "tacmonitor"
user = tacuser {
    pap = cleartext "tacpass"
    service = rbt-exec {
        local-user-name = "monitor"
    }
}

```

The secret you specify here must also be specified in the HP EFS WAN Accelerator when you set up TACACS+ server support. For detailed information, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

The **tacuser** is a monitor user as specified by **local-user-name**.

---

**NOTE:** The **chap**, **opap**, and **arap** variables can be specified in a similar manner, but only **pap** is needed.

---

**8.** Start the server by executing:

```
>/usr/local/sbin/tac_plus -C /usr/local/etc/tac_plus.conf
```

---

## Configuring RADIUS Authentication in the HP EFS WAN Accelerator

The following section provides the basic steps for configuring RADIUS authentication in the HP EFS WAN Accelerator.

## Configuring RADIUS Authentication

The following section describes the basic steps for configuring RADIUS authentication in the HP EFS WAN Accelerator.

You prioritize RADIUS authentication methods for the system and set the authorization policy and default user.

---

**IMPORTANT:** Make sure to put the authentication methods in the order in which you want authentication to occur. If authorization fails on the first method, the next method is attempted, and so forth, until all the methods have been attempted.

---

## Basic Steps

1. Configure the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
3. Navigate to the Setup: Authentication - General Settings page in the Management Console.
4. Define the default login and the authentication methods. Make sure you put the authentication methods in the order in which you want them to occur. If authorization fails on the first method, the next method is attempted, and so forth, until all the methods have been attempted.

**Figure 9-1.** Setup: Authentication - General Settings Page

The screenshot shows the Management Console interface. The top navigation bar includes links for Home, Setup, Reports, Logging, and Help, with 'Setup' being the active tab. The status is shown as 'Healthy'. On the right, it says 'Logged in as: admin [logout]'. The main content area has a sidebar with various configuration options like Optimization Service, Host Settings, Advanced Networking, etc. The current page is 'Authentication - General Settings'. It contains a note about the order of authentication methods. Under 'Authentication Methods', there are dropdown menus for Method 1 (Local), Method 2 (RADIUS), and Method 3 (TACACS+). Below that is an optional section for 'Advanced Authorization (Optional - For RADIUS/TACACS+ Only)' with fields for 'Authorization Policy' (set to 'Remote First') and 'Default User' (set to 'Admin'). At the bottom are 'Apply', 'Save', and 'Reset' buttons.

5. Navigate to the Setup: Authentication - Radius Servers page.
6. Specify the Server IP address, the authentication port, server key, time-out interval, retry interval, and, optionally, global settings.

**Figure 9-2.** Setup: Authentication - RADIUS Servers Page

The screenshot shows the 'Authentication - RADIUS Servers' configuration page. At the top, there's a navigation bar with links for Home, Setup, Reports, Logging, and Help. The status is shown as 'Healthy'. On the right, it says 'Logged in as: admin [logout]'. The main area has a title 'Authentication - RADIUS Servers' with a help icon. A note says: 'Configure your RADIUS authentication settings. This configuration is only necessary for appliances using RADIUS authentication.' Below this is a table with columns: Server IP, Port, Key, Timeout, Retries, and Enabled. A message 'No RADIUS servers.' is displayed. There are buttons for 'Remove Selected Servers', 'Enable', and 'Disable'. To the left of the table is a sidebar with a dark background containing a list of menu items under categories like Optimization Service, Host Settings, Advanced Networking, etc. One item, 'Authentications > RADIUS Servers', is highlighted with a blue arrow. At the bottom right of the main area are 'Save' and 'Reset' buttons.

7. Click Save.

## Configuring TACACS+ Authentication in the HP EFS WAN Accelerator

The following section provides the basic steps for configuring TACACS+ authentication in the HP EFS WAN Accelerator.

### Configuring TACACS+ Authentication

The following section describes the basic steps for configuring TACACS+ configuration in the HP EFS WAN Accelerator.

You prioritize TACACS+ authentication methods for the system and set the authorization policy and default user.

**IMPORTANT:** Make sure to put the authentication methods in the order in which you want authentication to occur. If authorization fails on the first method, the next method is attempted, and so forth, until all the methods have been attempted.

## Basic Steps

The following section describes the basic steps for configuring TACACS+ authentication in the HP EFS WAN Accelerator.

1. Configure the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
2. Connect to the Management Console. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
3. Navigate to the Setup: Authentication - General Settings page in the Management Console.
4. Define the authentication methods. Make sure you put the authentication methods in the order in which you want them to occur. If authorization fails on the first method, the next method is attempted, and so forth, until all the methods have been attempted.

**Figure 9-3.** Setup: Authentication - General Settings Page

The screenshot shows the 'Authentication - General Settings' page of the HP EFS WAN Accelerator Management Console. The left sidebar contains a navigation menu with items like Optimization Service, Host Settings, Advanced Networking, etc. The main content area has a title 'Authentication - General Settings' with a note: 'Check and modify your authentication settings. Please make sure to put the methods in the order you want authentication to occur.' Below this is a section titled 'Authentication Methods' with dropdown menus for Method 1 (Local), Method 2 (TACACS+), and Method 3 (RADIUS). There is also an 'Advanced Authorization (Optional - For RADIUS/TACACS+ Only)' section with dropdowns for Authorization Policy (Remote First) and Default User (Admin). At the bottom right are 'Apply', 'Save', and 'Reset' buttons.

5. Navigate to the Setup: Authentication - TACACS+ Servers page.

6. Specify the Server IP address, the authentication port, server key, time-out interval, retry interval, and, optionally, global settings.

**Figure 9-4.** Setup: Authentication - TACACS+ Servers Page

The screenshot shows the 'Authentication - TACACS+ Servers' page. At the top, there's a status bar with 'Status: Healthy' and 'Logged in as: admin [logout]'. On the left, a sidebar menu includes 'Optimization Service', 'Host Settings', 'Advanced Networking', 'Proxy File Service', 'Port Labels', 'Reports', 'Logging', 'Date & Time', 'Authentication' (with sub-options like 'General Settings', 'Account: Admin', 'Account: Monitor', 'RADIUS Servers', and 'TACACS+ Servers'), 'Licenses', 'Scheduled Jobs', 'Configuration Manager', 'Upgrade Software', and 'Start/Stop Services', 'Reboot Appliance', 'Shutdown Appliance'. The 'TACACS+ Servers' option is selected in the sidebar. The main content area has a heading 'Authentication - TACACS+ Servers' with a note: 'Configure your TACACS+ authentication settings. This configuration is only necessary for appliances using TACACS+ authentication.' Below this is a table with columns: Server IP, Port, Type, Key, Time-Out, Retries, and Enabled. A message 'No TACACS+ servers.' is shown. Below the table are buttons for 'Remove Selected Servers', 'Enable', and 'Disable'. To the right, there's a 'Global Settings' section with fields for Server Key, Timeout (set to 3 seconds), and Retries (set to 1). Buttons for 'Update Settings', 'Save', and 'Reset' are at the bottom. A modal dialog titled 'Add New TACACS+ Server:' contains fields for Server IP (10.2.0.2), Authentication Port (49), Authentication Type (PAP), Server Key (xxxxx), Timeout (30 seconds), Retries (2), and Enabled (True). A 'Save' button is at the bottom of the modal.

7. Click Save.



# Serial Cluster and Cascade Deployments

## In This Chapter

This chapter describes serial cluster and cascade deployments and summarizes the basic steps for configuring them. This chapter includes the following sections:

- ◆ “Serial Cluster Deployment,” next
- ◆ “Cascade Deployment” on page 111

This chapter assumes that you are familiar with the HP EFS WAN Accelerator Management Console (Management Console). For detailed information about the Management Console and how to use it, see the *HP Enterprise File Services WAN Accelerator Management Console User Guide*.

This chapter also assumes that you are familiar with the installation and configuration process for the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

This chapter provides the basic steps for serial cluster and cascade deployments. It does not provide detailed procedures. Use this chapter as a general guide for these deployments. If you need additional assistance, contact HP technical support at <http://www.hp.com>.

For detailed information about the factors you must consider before you deploy the HP EFS WAN Accelerator, see “[Design and Deployment Overview](#)” on page 11.

---

## Serial Cluster Deployment

You can provide increased optimization by deploying several HP EFS WAN Accelerators back-to-back in an in-path configuration to create a serial cluster.

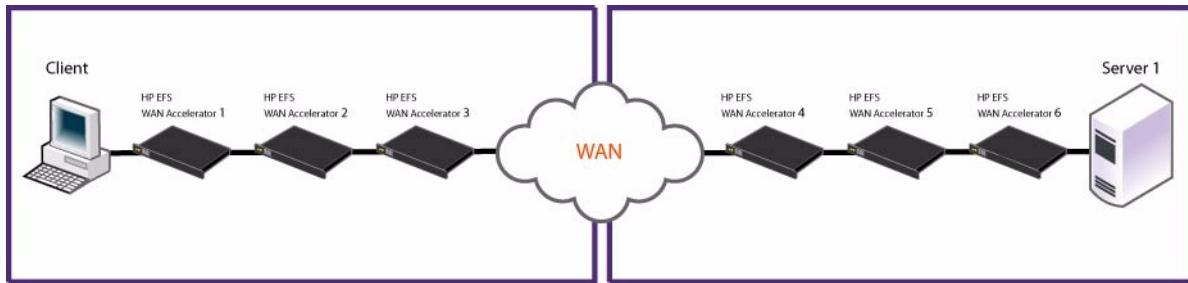
---

**IMPORTANT:** HP strongly recommends that only Series 5000 HP EFS WAN Accelerators are deployed in a serial cluster due to traffic loads.

---

Serial clustering operates in a *spill-over* mode where TCP connections beyond the capacity limit of one of the HP EFS WAN Accelerators in the cluster are automatically handled by the next HP EFS WAN Accelerator in a cluster. If one HP EFS WAN Accelerator fails, the next HP EFS WAN Accelerator automatically take over.

**Figure 10-1.** Serial Cluster



In this example, HP EFS WAN Accelerator1, HP EFS WAN Accelerator2, and HP EFS WAN Accelerator3 are configured so that they do not answer probes from each other and do not intercept inner connections from each other. Similarly, HP EFS WAN Accelerator4, HP EFS WAN Accelerator5, and HP EFS WAN Accelerator6 are configured so that they do not answer probes from each other and do not intercept inner connections from each other. The HP EFS WAN Accelerators are configured to perform auto-discovery so that they can find a peer HP EFS WAN Accelerator that is available and that is on the other side of the Wide Area Network (WAN).

You specify peering rules that when the HP EFS WAN Accelerator receives an auto-discovery probe it is passed through, accepted, or processed normally based on the sender of the probe, the client IP address and subnet, the server IP address and subnet, or the server port.

In a serial cluster when an HP EFS WAN Accelerator reaches its capacity limit, it stops intercepting new connections and passes them through to the next HP EFS WAN Accelerator that will intercept them. This process continues until there are no more HP EFS WAN Accelerators available in the cluster.

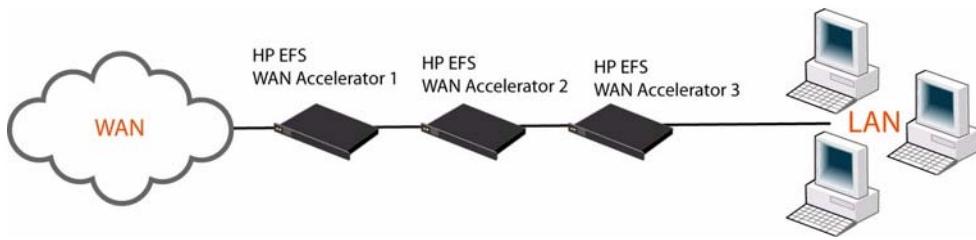
In serial cluster deployments:

- ◆ The peering rules table is a ordered list of rules and the first rule that matches the rule is applied.
- ◆ To avoid interceptions on inner connections created by other HP EFS WAN Accelerators in the same cluster, in-path rules are specified to pass-through connections originating from those HP EFS WAN Accelerators.

## A Basic Serial Cluster Deployment

The following example illustrates how to configure a cluster of three in-path HP EFS WAN Accelerators in a data center.

**Figure 10-2.** Serial Cluster in a Data Center



This example has the following parameters:

- ◆ HP EFS WAN Accelerator1 IP address is 10.0.1.1 on a /16
- ◆ HP EFS WAN Accelerator2 IP address is 10.0.1.2 on a /16
- ◆ HP EFS WAN Accelerator3 IP address is 10.0.1.3 on a /16

Each HP EFS WAN Accelerator is configured with in-path peering rules that prevent peering with another HP EFS WAN Accelerator in the cluster and with in-path rules that do not optimize connections originating from these HP EFS WAN Accelerators.

### To configure HP EFS WAN Accelerator1

1. On HP EFS WAN Accelerator1, connect to the CLI. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual*.
2. At the system prompt, enter the following set of commands:

```

SH1 > enable
SH1 # configure terminal
SH1 (config) # in-path peering rule pass peer 10.0.1.2 rulenumber 1
SH1 (config) # in-path peering rule pass peer 10.0.1.3 rulenumber 1
SH1 (config) # in-path rule pass-through srcaddr 10.0.1.2/32 rulenumber 1
SH1 (config) # in-path rule pass-through srcaddr 10.0.1.3/32 rulenumber 1
SH1 (config) # wr mem
SH1 (config) # show in-path peering rules
Rule Type Source Network Dest Network Port Peer Addr
----- -----
-
1 pass * * * 10.0.1.3
2 pass * * * 10.0.1.2
def auto * * * *

SH1 (config) # show in-path rules
Rule Type Source Addr Dest Addr Port Target Addr
Port
-----
-
1 pass 10.0.1.3/32 * -- --
2 pass 10.0.1.2/32 * -- --
def auto * * -- --
  
```

## To configure HP EFS WAN Accelerator2

1. On HP EFS WAN Accelerator2, connect to the CLI. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual*.

2. At the system prompt, enter the following set of commands:

```
SH2 > enable
SH2 # configure terminal
SH2 (config) # in-path peering rule pass peer 10.0.1.1 rulenum 1
SH2 (config) # in-path peering rule pass peer 10.0.1.3 rulenum 1
SH2 (config) # in-path rule pass-through srcaddr 10.0.1.1/32 rulenum 1
SH2 (config) # in-path rule pass-through srcaddr 10.0.1.3/32 rulenum 1
SH2 (config) # wr mem

SH2 (config) # show in-path peering rules
Rule Type Source Network Dest Network Port Peer Addr
----- -
1 pass * * * 10.0.1.3
2 pass * * * 10.0.1.1
def auto * * * *

SH1 (config) # show in-path rules
Rule Type Source Addr Dest Addr Port Target Addr
Port
----- -
1 pass 10.0.1.3/32 * * -- --
2 pass 10.0.1.1/32 * * -- --
def auto * * * -- --
```

## To configure HP EFS WAN Accelerator3

1. On HP EFS WAN Accelerator3, connect to the CLI. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command-Line Interface Reference Manual*.

2. At the system prompt, enter the following set of commands:

```
SH3 > enable
SH3 # configure terminal
SH3 (config) # in-path peering rule pass peer 10.0.1.1 rulenum 1
SH3 (config) # in-path peering rule pass peer 10.0.1.2 rulenum 1
SH3 (config) # in-path rule pass-through srcaddr 10.0.1.1/32 rulenum 1
SH3 (config) # in-path rule pass-through srcaddr 10.0.1.2/32 rulenum 1
SH3 (config) # wr mem

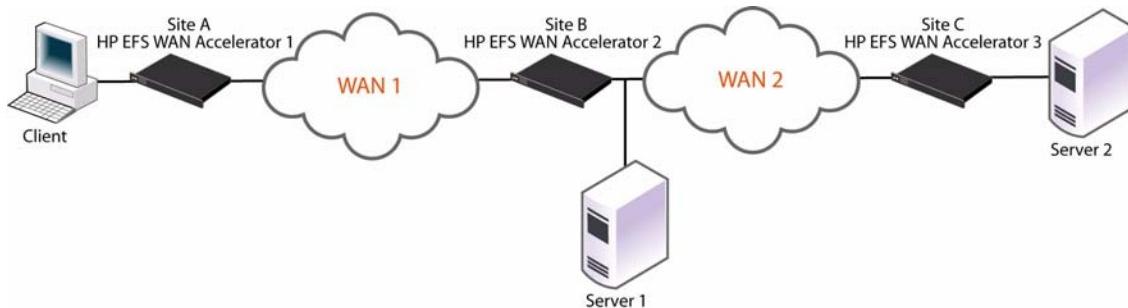
SH3 (config) # show in-path peering rules
Rule Type Source Network Dest Network Port Peer Addr
----- -
1 pass * * * 10.0.1.2
2 pass * * * 10.0.1.1
def auto * * * *

SH1 (config) # show in-path rules
Rule Type Source Addr Dest Addr Port Target Addr
Port
----- -
1 pass 10.0.1.2/32 * * -- --
2 pass 10.0.1.1/32 * * -- --
def auto * * * -- --
```

## Cascade Deployment

Cascade configurations enable multi-site deployments where the server end-points are located at intermediate sites and connections between the client and the server might pass through intermediate HP EFS WAN Accelerators to reach their final destination. HP EFS WAN Accelerators direct client-side HP EFS WAN Accelerator auto-discovery packets to the correct HP EFS WAN Accelerator end-point.

**Figure 10-3.** Cascade Deployment



When the Client connects to a server in Site B, HP EFS WAN Accelerator1 and HP EFS WAN Accelerator2 are optimizing the connection. When the Client connects to a server in Site C, HP EFS WAN Accelerator1 and HP EFS WAN Accelerator3 are optimizing the connection.

The following rules apply to cascade deployments:

- ◆ A cascade deployment can be created on either the client side or on the server side.
- ◆ In a cascade deployment, only pass-through peering rules are used.

## Peering Rules

Peering rules define what to do when an HP EFS WAN Accelerator receives an auto-discovery probe from another HP EFS WAN Accelerator.

In [Figure 10-3](#), Server1 is on the same LAN as HP EFS WAN Accelerator2 so connections from the client to Server1 should be optimized between HP EFS WAN Accelerator1 and HP EFS WAN Accelerator2. Concurrently, Server2 is on the same LAN as HP EFS WAN Accelerator3 and connections from the client to Server2 should be optimized between HP EFS WAN Accelerator1 and HP EFS WAN Accelerator3.

To configure this example, you do not need any rules on HP EFS WAN Accelerator1 or HP EFS WAN Accelerator3; you need to add peering rules on HP EFS WAN Accelerator2 to process normally connections going to Server1 and to pass all other connections so that connections to Server2 are not optimized by HP EFS WAN Accelerator2. You also need a default rule to pass through inner connections between HP EFS WAN Accelerator1 and HP EFS WAN Accelerator3 (by default connection to destination port 7800).

This example has the following parameters:

- ◆ Server1 IP address is 10.0.2.2 on a /24

```

SH2 > enable
SH2 # configure terminal
SH2 (config) # in-path peering rule pass rulenumber 1
SH2 (config) # in-path peering rule auto dest 10.0.2.0/24 rulenumber 1
SH2 (config) # in-path rule pass-through dstport 7800 rulenumber 1
SH2 (config) # wr mem

SH2 (config) # show in-path peering rules
Rule Type Source Network Dest Network Port Peer Addr
----- -----
 1 auto * 10.0.2.2/24 *
 2 pass * *
 def auto * *
----- -----
SH2 (config) # show in-path rules
Rule Type O N Source Addr Dest Addr Port Target Addr Port
----- -----
 1 pass - - * *
 2 def auto F A * *
----- -----

```

With peering rules, you do not define anything on HP EFS WAN Accelerator1 and can define an accept rule on HP EFS WAN Accelerator2 for probes going to Server1 and a pass-through rule for anything else. Connections going to Server1 would then be intercepted by HP EFS WAN Accelerator2, and connections going to anywhere else would be intercepted by another HP StorageWorks Enterprise File Services WAN Accelerator (for example, HP EFS WAN Accelerator3 for Server2).

## Fixed-Target Rules

If you choose not to define peering rules, you must define a fixed-target rule on HP EFS WAN Accelerator1 to go to HP EFS WAN Accelerator3 for connections to Server2. You must define a fixed-target rule on HP EFS WAN Accelerator3 to go to HP EFS WAN Accelerator1 for connections to servers in the same site as HP EFS WAN Accelerator1. If you have multiple branches that go through HP EFS WAN Accelerator2, you must add a fixed-target rule for each of them on HP EFS WAN Accelerator1 and HP EFS WAN Accelerator3.

# Glossary

**ARP.** Address Resolution Protocol. An IP protocol used to obtain a node's physical address.

**Bandwidth.** The upper limit on the amount of data, typically in kilobits per second (kbps), that can pass through a network connection. Greater bandwidth indicates faster data transfer capability.

**Bit.** A Binary digit. The smallest unit of information handled by a computer; either 1 or 0 in the binary number system.

**Blade.** One component in a system that is designed to accept some number of components (blades).

**CIFS.** Common Internet File System. CIFS is the remote file system access protocol used by Windows servers and clients to share files across the network.

**Database Cursor.** A record pointer in a database. When a database file is selected and the cursor is opened, the cursor points to the first record in the file. Using various commands, the cursor can be moved forward, backward, to top of file, bottom of file and so forth.

**Default gateway.** The default address of a network or Web site. It provides a single domain name and point of entry to the network or site.

**DHCP.** Dynamic Host Configuration Protocol. Software that automatically assigns IP addresses to client stations logging onto a TCP/IP network.

**Domain.** In the Internet, a portion of the Domain Name Service (DNS) that refers to groupings of networks based on the type of organization or geography.

**DNS.** Domain Name Service. System used in the Internet for translating names of network nodes into IP addresses. A Domain Name Server notifies hosts of other host IP addresses, associating host names with IP addresses.

**Ethernet.** The most widely used Local Area Network (LAN) access method.

**FDDI.** Fiber Distributed Data Interface. A set of American National Standards Institute (ANSI) protocols for sending digital data over fiber optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits) per second. FDDI networks are typically used as backbones for Wide-Area Networks (WANs).

**Filer.** An appliance that attaches to a computer network and is used for data storage.

**Gateway.** A computer that acts as an intermediate device for two or more networks that use the same protocols. The gateway functions as an entry and exit point to the network. Transport protocol conversion might not be required, but some form of processing is typically performed.

**Gigabit Ethernet.** An Ethernet technology that raises transmission speed to 1 Gbps (1000 Mbps).

**Hashing.** Producing hash values for accessing data or for security. A hash value, is a number generated from a string of text. The hash is substantially smaller than the text itself and it is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

**Heartbeat.** A repeating signal transmitted from one appliance to another that indicates that the appliance is operating.

**Heuristic.** A method of problem solving using exploration and trial and error methods. Heuristic program design provides a framework for solving the problem in contrast with a fixed set of rules (algorithmic) that cannot vary.

**Host.** A computer or other computing device that resides on a network.

**Host address.** The IP address assigned to each computer attached to the network.

**Host name.** Name given to a computer, usually by DNS.

**HSRP.** Hot Standby Routing Protocol. HSRP is a routing protocol from Cisco that provides backup to a router in the event of failure. Using HSRP, several routers are connected to the same segment of an Ethernet, FDDI or token-ring network and work together to present the appearance of a single virtual router on the LAN. The routers share the same IP and MAC addresses, therefore in the event of failure of one router, the hosts on the LAN are able to continue forwarding packets to a consistent IP and MAC address. The process of transferring the routing responsibilities from one device to another is transparent to the user.

**HTTP.** Hypertext Transport Protocol. The protocol used by Web browsers to communicate with Web servers.

**HTTPS.** Hypertext Transport Protocol Secure. The protocol for accessing a secure Web server. Using HTTPS directs the message to a secure port number to be managed by a security protocol.

**Interface.** The point at which a connection is made between two elements, systems, or devices so that they can communicate with one another.

**Internet.** The collection of networks tied together to provide a global network that use the TCP/IP suite of protocols.

**IP.** Internet protocol. Network layer protocol in the TCP/IP stack that enables a connectionless internetwork service.

**IP address.** In IP version 4 (IPv4), a 32-bit address assigned to hosts using the IP protocol. Also called an Internet address.

**IPsec.** Internet Protocol Security Protocol. A set of protocols to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. For IPsec to work, the sending and receiving devices must share a public key.

**Latency.** Delay between a request being issued and its response being received.

**Layer-4.** A communications protocol (called the transport layer) responsible for establishing a connection and ensuring that all data has arrived safely. The application delivers its data to the communications system by passing a stream of data bytes to the transport layer along with the socket (the IP address of the station and a port number) of the destination machine.

**MAPI.** Messaging API. A programming interface from Microsoft that enables a client application to send and receive mail from Exchange Server or a Microsoft Mail (MS Mail) messaging system. Microsoft applications such as Outlook, the Exchange client, and Microsoft Schedule use MAPI.

**Microsoft Exchange.** Messaging and groupware software for Windows from Microsoft. The Exchange server is an Internet-compliant messaging system that runs under Windows systems and can be accessed by Web browsers, the Windows In-box, Exchange client or Outlook. The Exchange server is also a storage system that can hold anything that needs to be shared.

**Netmask.** A 32-bit mask which shows how an Internet address is divided into network, subnet, and host parts. The netmask has ones in the bit positions in the 32-bit address which are used for the network and subnet parts, and zeros for the host part. The mask must contain at least the standard network portion (as determined by the class of the address), and the subnet field should be contiguous with the network portion.

**Neural Network.** A modeling technique based on the observed behavior of biological neurons and used to mimic the performance of a system. It consists of a set of elements that start out connected in a random pattern, and, based upon operational feedback, are molded into the pattern required to generate the required results. It is used in applications such as robotics, diagnosing, forecasting, image processing and pattern recognition.

**NFS.** Network File System. The file sharing protocol in a UNIX network.

**NIS.** Network Information Services. A naming service that allows resources to be easily added, deleted or relocated.

**OSPF.** Open Shortest Path First. An interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-

state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links. It also sends the complete routing structure (topography).

**Packet.** A unit of information transmitted, as a whole, from one device to another on a network.

**Probe.** A small utility program that is used to investigate, or test, the status of a system, network or Web site.

**Policy.** Routing and Quality of Service (QoS) scheme that forwards data packets to network interfaces based on user-configured parameters.

**Port.** A pathway into and out of the computer or a network device such as a hub, switch, or router. On network devices, the ports are for communications, typically connecting Ethernet cables or other network devices.

**Router.** A device that forwards data packets from one LAN or WAN to another. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.). Routers work at Layer-3 in the protocol stack, whereas bridges and switches work at the Layer-2.

**SMB.** Server Message Block. A message format used by DOS and Windows to share files, directories and devices. There are also a number of products that use SMB to enable file sharing among different operating system platforms. A product called Samba, for example, enables UNIX and Windows machines to share directories and files.

**SNMP.** Simple Network Management Protocol. A network protocol that provides a way to monitor network devices, performance, and security and to manage configurations and collect statistics.

**Switch.** A network device that filters and forwards frames based on the destination address of each frame. The switch operates at Layer-2 (data link layer) of the Open System Interconnection (OSI) model.

**TCP.** Transmission Control Protocol. The error correcting Transport layer (Layer-4) in the TCP/IP protocol suite.

**TCP/IP.** Transmission Control Protocol/Internet Protocol. The protocol suite used in the Internet, intranets, and extranets. TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. TCP/IP is a routable protocol, and the IP part of TCP/IP provides this capability.

# Index

## A

Architecture, overview of 9  
 Authentication, overview of 97  
 Auto-discovery rules, overview of 13  
 Autodiscovery, configuring with CDP 60  
 Autodiscovery, configuring with PBR 57

## B

Bypass mode, overview of 13

## C

Cascade clusters, overview of 111  
 CDP, overview of 46  
 Connection forwarding  
     configuring using the CLI 44  
     configuring using the Management Console 42  
     failover deployment, configuring 41  
     neighbors in 40  
     overview of 39

## D

Designing your deployment 11

## E

Ethernet network compatibility 4

## F

Failover support, overview of 13  
 Fail-through support 13  
 Fixed target rules, overview of 13

## G

GRE 65

## H

HP

    storage web site 7  
 Hybrid deployment, configuring 35  
 Hybrid deployment, overview of 26

## L

Layer-4 switch, configuring 26  
 Load balancing, configuring 26  
 Logical in-path deployment

load balanced, Layer-4 switch deployment,  
     configuring 26  
 WCCP, overview of 26

## M

Multicast in WCCP 65

## N

Neighbors, overview of 40

## O

Online documentation 6  
 Optimization, overview of 13  
 Out-of-path deployment  
     failover support, configuring 30  
     overview of 29  
     static cluster, configuring 33

## P

Pass-through rules, overview of 13

## PBR

    asymmetrical deployment, configuring 49  
 CDP and autodiscovery, configuring 60  
 client-side deployment, configuring 50, 54  
 client-side, inside router deployment,  
     configuring 55

    configuring using the Management Console 51  
 connecting HP EFS WAN Accelerator for 48  
 how it works with Cisco 6500 47  
 overview of 46  
 single subnet deployment, configuring 49  
 symmetrical deployment, configuring 57  
 troubleshooting 60, 62  
 VLAN deployment, configuring 55

## PFS

    broadcast mode 85  
 configuration requirements 88  
 configuring using the Management Console 89  
 how does it work? 86  
 local mode 85  
 overview of 83  
 stand-alone mode 86

terms 84  
Physical in-path deployment  
overview of 12  
server-side, configuring 21  
server-side, one to one, configuring 22  
two routing points, configuring 20

**R**  
**RADIUS**

configuring a RADIUS server 98  
configuring the appliance 101  
overview of 97  
Related reading 6

**S**  
Scalable Data Referencing, overview of 10, 13  
Serial cluster, configuring 109  
Share synchronization, definition of 85  
Share, definition of 85  
Static cluster deployment, configuring 33

**T**  
**TACACS+**  
configuring a TACACS+ server 100  
configuring in the appliance 103  
overview of 97  
Transaction Acceleration, overview of 10  
Transaction Prediction, overview of 11

**U**  
Unicast in WCCP 65

**V**  
**Virtual in-path deployment**  
hybrid, configuring 35  
hybrid, overview of 26  
overview of 25  
Virtual Window Expansion, overview of 10

**W**  
**WCCP**  
basic configuration 68  
basic steps for configuring 65  
CLI commands for 66  
configuring using the Management Console 70  
dual deployment, configuring 76  
failover support, configuring 81  
load balancing, configuring 81  
multicast, configuring 80  
overview of 26, 63, 64  
security, configuring 79  
specific redirection, configuring 81  
TCP port redirection, configuring 80  
troubleshooting 82